UNIVERSITY OF ZAGREB
FACULTY OF ORGANIZATION AND INFORMATICS

Mario Žgela, M Sc

DEVELOPMENT OF METHODOLOGY FOR COMPUTER ASSISTED INFORMATION SYSTEMS AUDITING

DOCTORAL DISSERTATION

Varaždin, 2010.

UNIVERSITY OF ZAGREB
FACULTY OF ORGANIZATION AND INFORMATICS
VARAŽDIN

Supervisor: Dr. sc. Zdravko Krakar, university professor

Content

List of Figures ..... **iii**

List of Tables ..... **iv**

Foreword **1**

1. Introduction **3**

1.1 Description of a Problem 3
1.2 Objectives and Hypotheses 5
1.3 Terminology 7

2. Analysis of Some Cases Resulting in Significant Losses or Bankruptcies **11**

2.1 Analysis of Barings Bank Case 12
2.2 Analysis of Allied Irish Banks Case 14
2.3 Analysis of Riječka banka Case 16
2.4 Analysis of Societe Generale Case 19
2.5 Analysis of Madoff Case 21
2.6 Conclusions on Causes 22

3. Risks in Development and Use of Information Systems **25**

3.1 Importance of Information Systems Management 25
3.2 Importance of Risk Based Approach 25
3.3 Operational Risk and Basel II 28
3.4 Operational Risk and FED 32

4. Identification and Analysis of Existing Frameworks and Approaches for Information Systems Auditing **35**

4.1 Approach of Information Systems Audit and Control Association 36
4.1.1 Information Systems Standards, Guidelines and Procedures for Auditing and Control Professionals *38*
4.1.2 Control Objectives for Information and Related Technologies (COBIT) *41*
4.2 Bank for International Settlements Approach 46
4.3 Federal Reserves Bank (FED) Approach 55
4.4 Approach of Croatian National Bank 60
4.4.1 The Banking Law *60*
4.4.2 Decision on Adequate Information System Management *63*
4.5 Conclusion on Existing Frameworks and Approaches 67

5. Analysis of Particular Methods for Computer Assisted Information Systems Auditing **73**

5.1 Benford's Law 77
5.2 Selection 77
5.3 Join 79
5.4 Summarization 80

5.5 Stratification 81
5.6 Duplication 82
5.7 Rounded values 82
5.8 Conclusion on Methods for Computer Assisted Auditing of Information Systems 83

6. The Role of Benford's Law in Information Systems Auditing 86

6.1 Definition and Description 86
6.2 Intuitive Explanation 90
6.3 Properties of Conformance of Number Set to Benford's Law 92
6.4 Invariance Property of Benford's Law 93
6.5 The First Digit Test 96
6.6 The First Two Digits Test 99
6.7 The First Three Digits Test 105
6.8 The Second Digit Test 110
6.9 Benford's Law Conformance Criteria 113
6.9.1 Z-statistics 114
6.9.2 Chi-square (χ^2) 116
6.9.3 Mean absolute deviation 117

7. Design and Verification of Computer Assisted Information Systems Auditing Methodology 119

7.1 Meta-Model of Computer Assisted Information Systems Auditing Methodology (CAISAM) 120
7.2 Model of CAISAM Based on Benford's Law 123
7.3 Verification of Designed Methodology 134
7.3.1 Description of Cross-border Payments System 134
7.3.2 Requirements on Cross-border Payments System Auditing 136
7.3.3 Cross-border Payments System Auditing 138
7.4 Evaluation of Developed Methodology 166

8. Improvement of Computer Assisted Auditing Tools Functionality and Auditing Quality 170

8.1 Audit Phases and Necessary Characteristics of Computer Assisted Auditing Tools 171
8.1.1 Audit Planning 171
8.1.2 Audit Execution 176
8.1.3 Audit Documenting 184
8.1.4 Reporting 185
8.2 Improvement of Auditor’s Work Quality 185
8.3 The Challenges in Implementation of Computer Assisted Auditing Tools 190

9. Achieved Objectives and Confirmation of Hypotheses 195

10. Conclusion 198

11. References 201

List of Figures

Figure 1. First digit probabilities of actual data set and Benford's Law probabilities 98
Figure 2. First two digits probabilities of observed data set (Po) and Benford's Law probabilities (PBL) 103
Figure 3. First two digits - actual (Po) and Benford's Law (PBL) proportions 107
Figure 4. First three digits - "Spikes" and "sinks" 109
Figure 5. The second digit frequencies 111
Figure 6. Normal distribution and different significance levels with corresponding cut off values 114
Figure 7. CAISAM Meta-model 121
Figure 8. CAISAM Model 125
Figure 9. Frequency deviation from Benford's Law for first digit for all payments in original currency 144
Figure 10. Frequency deviation from Benford's Law for first two digits for all payments in original currency 156
Figure 11. Frequency deviation from Benford's Law for first two digits of original currency payments for goods 159
Figure 12. Actual (PRs) and Benford's Law proportions (PRo) of original currency payments from abroad for goods 160

List of Tables

Table 1. Methods and corresponding objectives, inputs and outputs 85
Table 2. Probabilities of each digit on the first position in number according to Benford's Law (base b=10) 87
Table 3. Probabilities of each digit on the second position in number according to Benford's Law 88
Table 4. Distribution of first digit – compiled by Frank Benford 89
Table 5. Multiplication of number set conforming to Benford's Law by a constant 95
Table 6. Frequencies and probabilities for first digits in original 95
and multiplied number sets 95
Table 7. The first digit frequencies of example invoice totals 97
Table 8. The first two digit frequencies of invoice total amounts 101
Table 9. Focus on digits with excessive frequencies 103
Table 10. The first two digits test for received invoices 106
Table 11. First three digits combinations that follow from first two digits combinations from Table 10 108
Table 12. The second digit frequencies in contracted yearly insurance policies 111
Table 13. Stratification according to 7 days strata periods applied on transaction dates 141
Table 14. First digit (d) analysis of amounts in original currency for all payments 142
Table 15. Specific rounded and duplicated payments amounts (deposits) 146
Table 16. Specific rounded and duplicated payments amounts (currency exchange) 146
Table 17. Specific rounded and duplicated payments amounts (deposits) 148
Table 18. Specific rounded and duplicated payments amounts (currency exchange) 148
Table 19. Summarization based on month-year period and bank code 149
Table 20. Second digit (d) analysis of amounts in original currency payments 150
Table 21. The most frequent payment purposes ("code of pp") with digit "0" on 2nd position in payment amount 151
Table 22. Summarization of payments with purpose code 340 and specific amount set 152
Table 23. Summarization of payments with purpose code 110 and specific amount set 153
Table 24. The most frequent payments purposes ("code of pp") with digit "5" on 2nd position in payment amount 154

Table 25. Rounded values of selected codes of payments with second digit “5” 155
Table 26. First digit (d) analysis of amounts in original currency payments for goods 158
Table 27. First digit (d) analysis of amounts in original currency payments from abroad for exported goods 160
Table 28. Comparison of deviations between payments for goods 161
Table 29. Selected results of the first three digits Benford’s Law test 163
Table 30. Methods used in CAISAM 168

Foreword

After the introductory notes, this doctoral dissertation analyses some known business cases resulted in significant losses or bankruptcies. Some of those cases caused regional and even global economic disturbances and fostered global economic crisis. Also, importance of risks management in development, use and maintenance of information systems is emphasized.

One of key challenges is the fact that the amounts of data stored in databases of business systems continuously increases which leads to the conclusion that it becomes harder to detect fraud, omissions and errors. If control processes are based on inappropriate methods and tools it is often impossible to perceive mentioned flaws in business activities.

It is clearly stated that information systems auditing one of key issues that could prevent or mitigate information systems risks and that should be covered in more details.

Thesis describes problems and challenges in information systems auditing, existing frameworks, approaches and methods while focusing on development of specific computer assisted information systems auditing methodology (CAISAM). Although certain concepts, frameworks and even legal frameworks for information systems auditing exist for years, clear need for detailed, standard and repeatable methodology is identified. It is explained that without detailed methodology, information systems audits are non-standard, non-repeatable, inconsistent i.e. auditors perform audits in accordance with their personal preferences. CAISAM is thoroughly described, verified and evaluated on available cross border payment system transactions. Although some other methods are used within methodology, Benford's Law is used as a fundamental. It is shown how Benford's Law tests of first, second, first two and first two digits can be extremely helpful in information systems auditing and investigating possible frauds, omissions and errors.

It is also explained what are the possible improvements in each audit phase while focusing on characteristics which can lead to increased efficiency of computer assisted auditing tools.

Information systems auditing issues, and especially those related to fraud, omissions and errors, are for a long time in the focus of my interest. This doctoral dissertation is my humble contribution to improvement of information systems auditing.

Although I devoted significant time and resources while producing this thesis, what my spouse and children noticed occasionally, this work would never be done without the help of experts and friends, who are smarter and wiser than me, and family. Firstly, I would like to thank to my mentor professor Zdravko Krakar, Ph D, who despite his extremely full schedule managed to give numerous valuable advices and guidance on how to produce this thesis and especially how to improve development of CAISAM.

Somewhere in 1999., Mr Petar Ćurković, the president of Information Systems Audit and Control Association, former IT executive director and chief security officer in Croatian National Bank, introduced me with the notion of Benford's Law in data analysis and audit. His amazing and stunning clear comprehension of very complex ideas and surprisingly quick recognition of proper courses were of immense importance in finalizing of this thesis.

Finally, I would like to thank to my wife Ivana and my three children who had enough understanding for my daily and nightly activities on this thesis. I promise, we will spend more time together!

Mario Žgela

1. Introduction

1.1 Description of a Problem

Effective management of organisation's information system is of great importance to its development, success and even survival. In global information society, in which decision making process relies on adequate, timely and correct data, this importance comes from:

- Increasing dependence on information and the information systems which ensure this information
- Increasing risks and vulnerabilities and a large set of threats, such as cyber threats, information warfare, omissions and errors based on inappropriate usage of information systems
- Cost of the present and future investments and expenditures in information systems
- Technologies potential to significantly change organisations and business practices, business processes, create new opportunities for profit gaining and growth and to dramatically reduce costs
- Possibility of committing frauds, embezzlements and mistakes through unauthorized or uncontrolled use of information systems and/or information technology.

Since importance of information system was recognized, a number of management approaches were introduced in order to improve its efficiency, correctness and effectiveness. One of extremely important management approaches is information systems audit. Modern information systems audit is practically on the scene since the early beginning of usage of computer technology in the institutions and organizations.

Although nowadays there are widely accepted frameworks and approaches for information systems auditing, in the practice lot of variations in actual audits exist. There are numerous methods that are demanded by frameworks, approaches and legal acts that are applied in different ways in audit process. Also, although legal acts are based on certain de facto industrial standards in information systems auditing, they have their own specifics, covering some aspects more or less in details giving stress on certain areas depending on experience, risk assessment and business environments they suppose to cover. If legal act concerning

information systems auditing is to cover banking industry, then it will have focus on risks that are more related to banks. Obviously, data integrity should be in centre of such act, since most of frauds, losses and bankruptcies were committed because of lack of controls in access privileges, access control and authentication domains. Also, investment banking, foreign exchange and treasury applications are to be audited especially thoroughly since their usage is especially risky and may bring extreme profits but also extreme losses.

Additionally, the amounts of data stored in contemporary databases of business systems grow exponentially. Immense data growth leads to the fact that it becomes harder and harder to identify possible frauds, omissions and errors during the audit conduct. If during the audit conduct classical audit approaches are used it is often impossible to perceive mentioned flaws in business activities, especially if flaws are just in its initial period. It is usually possible to note these flaws only after longer period of time when losses become enormous, as it is shown in chapter 2. Additionally, as it is explained in chapter 2, frauds based on computer technology represent new category of criminality.

In order to eliminate or at least to mitigate these problems, auditing and regulatory communities propose necessity to use adequate risk management approaches and frameworks as it is shown in chapters 3 and 4 respectively. Since manual procedures are inadequate because of huge amounts of data residing in contemporary databases of business entities, modern and sophisticated methods based on computer assisted auditing tools, as it is shown in chapters 4 and 5, are becoming indispensable in audit conduct. So, since management of data is of crucial importance for any business and all major frauds were based on data manipulation, as shown in chapter 2, data review must be indispensable component of each audit. As data volumes in databases are usually extremely large commencing manual data review is out of question. Computer assisted auditing methods and tools may be of enormous help in achieving more detailed data audit and widening the scope covered by the audit process. These methods and tools may ensure better efficiency, cover more or all data and increase correctness of audit work. However, although methods and tools are developed and existing for some years, they are very often misused and do not help in prevention and development of early warning system for discovery of frauds, omissions and errors within information systems of business entities.

Furtherly, although data auditing is indispensable component of each auditing process, use of computer assisted auditing tools and wide variety of methods for data auditing are promoted and described by use of authorities, still there is no accepted computer assisted auditing methodology. Without strictly established methodology each audit is commenced with different methods, their order and mutual relationships so conclusions on errors, omissions or frauds may be based on different assumptions. One of outcomes of such situation is that auditors use different methods even if the same auditing environment is regarded. Furthermore, two data audits of the same data set within the same business entity are usually not comparable and with different conclusions. Adequate data auditing methodology based on computer assisted auditing methods is indispensable for improvement of audit process and adequate use of computer assisted auditing tools. Execution of complete and efficient audit is not possible if adequate and accepted methodology for computer assisted auditing is not developed and applied on business data residing within information system databases.

1.2 Objectives and Hypotheses

In this doctoral thesis, risks in development and application of information systems and importance of information systems management in improvement of business system as a whole will be explained. Some cases of losses and bankruptcies based on faults in control and audit, especially because of lack of computer assisted audit, will be analysed. According to importance of operating risk in business environment, Basel II and FED approaches will be briefly analyzed. Analysis of existing methods and approaches for information systems audit will be accomplished.

The necessity for definition of adequate methodology for computer assisted audit will be explained. The problem of development of methodology for computer assisted auditing will be addressed because that field of audit is not thoroughly investigated and systematized so adequate methodology with clearly defined methods, way of method’s application and sequence of their execution does not exist. Properties and advantages of certain methods and their application in methodology for computer assisted auditing will be thoroughly explained. Benford's Law, as a base method of methodology, will be explained and analysed in more details. Importance of Benford's Law as a link between different methods in methodology for computer assisted audit will be stressed.

Meta-model of computer assisted information systems auditing methodology will be developed. The principal result of this work will be particular developed methodology that will encompass list, mutual relationships and ways of usage of specific methods. Model of this particular methodology will be designed. Developed methodology will be applied on foreign payments system and evaluated. Especially detailed will be explanation of ways and possibilities of Benford's Law use and its combining with other methods of methodology within foreign payment system audit. The adequacy of developed methodology will be checked within audit of foreign payment transactions system in Republic of Croatia. Research will be based on data of payment transactions generated by commercial and central banks in Croatia. Results will be interpreted in detail and developed methodology evaluated.

Properties and instructions for adequate usage of computer assisted auditing tools will be defined as well as description of possible implementation problems. It will be shown that existing computer assisted auditing tools can ensure only partial support in audit process and that they need to be further improved.

To summarize, the objectives of this paper are to:

- identify needs for application of computer assisted information systems auditing
- identify, systematize and evaluate existing approaches, frameworks and methods for computer assisted information systems auditing
- check the possibility of Benford's Law usage as backbone of methodology for computer assisted information systems auditing
- define methods that will form methodology
- set up a meta-model and model of computer assisted information systems auditing methodology
- define the sequence and interconnections between specific methods
- apply developed methodology on real data sets and prove that developed methodology improves audit conduct
- give recommendations for extension of functionality of computer assisted auditing tools
- point out the needs for further research

The first hypothesis of this paper states that it is possible to develop computer assisted information systems auditing methodology (CAISAM).

The second hypothesis is that auditing process may be improved if developed CAISAM is applied.

In order to prove these hypotheses, existing approaches and frameworks for information systems auditing are going to be identified. Since there is no known methodology for computer assisted information systems auditing, one very usable methodology will be developed. That methodology will be based on Benford's Law which characteristics will be explained in details. Also, other supportive methods that form methodology will be thoroughly described and explained. Developed CAISAM will be verified on audit activity of real-world data set. It will be shown that this methodology is very effective in audit conduct and that audit process is significantly improved if such methodology is used.

Additionally, other important recommendations and instructions for application of computer assisted auditing tools in auditing process will be explained.

1.3 Terminology

The auditing activity is used in various fields of human activity. Whenever the need for after the fact check-up appears, it is most likely that some kind of audit will be performed.

According to a Merriam-Webster's dictionary, term audit denotes**:** "1. a: a formal examination of an organization's or individual's accounts or financial situation, b: the final report of an audit 2. a methodical examination and review".

Information Systems Auditing and Control Association, a world leading organization in fields of information systems audit and control, defines audit as "formal inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met."

Institute of Internal Auditors defined a term "internal auditing" as "an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic,

disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."

For the purpose of this work, term audit considers periodic reviews of risks and implemented controls, evaluation of threats and vulnerabilities, recovering of fraudulent activities and verification if implemented controls are appropriate.

It is well known that business system and its underlying and supportive information system (IS) are deeply interleaved. Usually it is not possible to easily mark off the borderline between these two systems. Simply speaking, there is no business system without information system. That is why information systems auditing and business conduct auditing are terms that can not be fully and clearly separated. Practically, any business audit will include more or less information system audit activities. Also, information systems together with business systems are becoming heavily dependent on information technology (IT). Further to that, information system audit has to include audit of information technology which serves as a backbone of information system.

Information systems audit must be a part of the business audit process, which is one of the enablers of eligible management of business entities. Although there is no generally accepted definition of information systems auditing, it can be stated that it is "the process of collecting and evaluating evidence to determine whether a computer system (information system) safeguards assets, maintains data integrity, achieves organizational goals effectively and consumes resources efficiently." [23, page 1].

Furtherly, the broad definition of computer assisted auditing software includes any software that can be used by the auditor to perform audits and to achieve the goals of auditing [24, page 1]. According to that rather general definition, computer assisted auditing software can be broadly categorized as follows:

- software for preparation of audit programme and audit execution follow up
- penetration testing and network analysis software
- operating systems and database management systems configuration analysis software
- application code testing software
- business process analysis software

- data audit software

That categorization encompasses wide variety of software packages including but not limited to spreadsheets like Excel, word processors (Word), query by example tools, client development environments (Access), statistical tools (SAS) etc.

Data audit software is the most often used of all above mentioned categories. That software is capable of selecting and extracting data from databases or flat files, performing different queries and usually has built in functions which can be very useful in data audit and analysis. In practice and literature term "computer assisted auditing software" is usually equalled to data audit software. However, even third expression is used very often: "computer assisted auditing tools" (CAAT). For the purpose of this paper, term "data audit software" from above categorization will be equalled with terms "computer assisted auditing tools" and "computer assisted auditing software". Therefore, terms "data audit software", “computer assisted auditing tools” and “computer assisted auditing software” will be used interchangeably, as a synonym.

In literature the abbreviation CAAT also stands for "computer assisted auditing techniques". A term "computer assisted auditing techniques" includes techniques and methods for computer assisted auditing. A word “technique” in this expression encompasses not only techniques in their narrower sense but also methods. This is so, because in literature on computer assisted auditing techniques and tools, words “technique” and “method” are also used interchangeably. However, word “technique” was included in the acronym CAAT. And finally, it can be stated that each computer assisted auditing tool (or software) is based on specific computer assisted auditing techniques and methods. Also, in literature term “computer assisted auditing tools and techniques” (CAATT) is used as a compounding term for both “computer assisted auditing tools” and “computer assisted auditing techniques”. In [3] "CAATTs are defined as computer-based tools and techniques which permit auditors to increase their personal productivity as well as that of the audit function". This is quite very broad definition, similar to definition in [24, page 1] already mentioned in this paper. Further in [3] it is stressed that computer is the ideal tool for sorting, searching, matching and performing various types of tests and mathematical calculations on data. CAATTs allow

auditors to probe data and information interactively and to react immediately to the findings by modifying and enhancing the initial approach.

This explanation narrows the definition of CAATTs to software that includes specific data analysis techniques and methods which enable adequate data audit and improve overall audit process.

To conclude, computer assisted auditing in this paper is defined as a process of data extraction, examination and analysis in order to identify exceptions, potential fraud, omissions or errors. That process always includes use of certain computer assisted auditing tools and computer assisted auditing techniques and methods.

2. Analysis of Some Cases Resulting in Significant Losses or Bankruptcies

In last decade IT solutions changed not only the ways business entities perform their businesses, but also significantly shifted risk areas, types of errors and omissions and even methodologies of certain types of criminal activities.

During 1990's and 2000's, the general public was witnessing bankruptcies or significant financial losses of a number of companies. In some banks, the amount of losses skyrocketed and even almost resulted in complete country's bankruptcy, because state economies are largely dependent on banks. Usually, losses and bankruptcies are caused by inadequate risk control mechanisms especially in area of operational risks. Financial losses and even bankruptcies resulted from inadequate use of information systems, specifically information and computer technologies. In some cases, it is evident that losses resulted from activities which fall into category of computer criminal.

Banking systems are specifically vulnerable to so-called "domino effect". The domino effect is a chain reaction occurring after a small change causes a similar change in neighbouring environment, which then in turn cause another similar change in its close environment, and so on. In economy, specifically in banking industry, domino effect is phenomenon in which losses or bankruptcy of one (often smaller) business entity causes a number of losses and bankruptcies of other business entities. It is of systemic importance to prevent domino effects in baking industry, which is one of major tasks of central banks and financial supervising and auditing authorities. Unfortunately, some recorded losses and bankruptcies were caused not only by local failures but also by macro and even global negative economic impacts. What should be in focus of supervisors, auditors, legal systems managing financial industry, management boards and information systems management is that in certain cases inappropriate information systems management can result in such systemic domino effects.

2.1 Analysis of Barings Bank Case

Nowadays, it is completely clear how Nick Leeson, head of front and back offices in Barings Bank Singapore branch, conducted otherwise prohibited actions which finally lead to bank's bankruptcy.

Leeson engaged in unauthorised trading in futures and options. Leeson was supposed to be arbitraging, seeking to profit from differences in the prices of Nikkei 225 futures contracts listed on the Osaka Securities Exchange in Japan and the Singapore International Monetary Exchange. Such arbitrage involves buying futures contracts on one market and simultaneously selling them on another at higher price. Since everyone tries to take advantage of a price difference on a publicly traded futures contract, the margins on arbitrage trading are quite small. Consequently, the volumes traded must be very large in order to earn any substantial profit because trader is buying something at one market while selling the same good at another market at the same time. Consequently, almost all risks are hedged and this strategy is not very risky so it certainly would not bankrupt the bank. However, instead of daily hedging bank's trades, Leeson gambled on the future direction of the Japanese markets. He hoped contract prices will go up in the future. In this instance, even a percent change of the price could create millions worth profit or loss.

According to Board of Banking Supervision of Bank of England report on Barings Bank Collapse, Leeson managed that details about account 88888 which, according to his own words, "related to errors" were omitted from report regularly sent to bank's headquarters in London. He managed to do that because he had IT team under his line of control. Leeson gave instructions to application programmers how to change report application. Interestingly enough, programmers did not perform any felony - there was no agreement between them and Leeson. However, programmers were only executing Leeson's orders without many questions. Unfortunately, transactions on account 88888 held details on Leeson's unauthorized trading.

By 31st of December 1994 he had caused losses on this account of around 208 million pounds Sterling. However, he managed to make false representation that he was in fact making profits for the bank. Moreover, Leeson was recognized as an extremely successful trader in Barings Bank.

Leeson concealed unauthorised trading by a number of methods. Apart from suppression of account 88888 from Barings in London, he submissioned false reports to London which included the misrepresentation of the profitability of his trading. He also presented to management a number of false trading and accounting transactions.

Auditing activities performed in 1995 showed losses skyrocketed to more than 800 million pounds Sterling, which equalled bank's capital. Soon afterwards, bank went bankruptcy and it was taken over by Dutch banking group ING for 1 pound Sterling.

Double check procedures were absent. If London headquarter conducted regular reconciliation and report check with other available information, attention would be drawn on incomplete Singapore branch reports reasonably quickly.

Further analysis of this case questioned the role and usefulness of internal audit department. In one of its earlier draft reports, internal audit suggested regular reconciliation of front and back offices data in Singapore branch. However, that was not accepted by the manager responsible for front and back office, i.e. Nick Leeson himself. Leeson justified his refusal of internal audit recommendation and commented that reconciliation would waste time and workforce resources. Senior managers accepted his justification, so recommendation was excluded from final report. Finally, internal audit department expressed serious concern because Leeson managed both front and back offices. Although the internal audit did not find out unauthorised trading, their report covered specific recommendations in the area of separation of duties in Leeson’s case. Unfortunately, these recommendations were never implemented in practice. The fact that Leeson was permitted to stay in charge of both front back office was a very serious failure.

Furthermore, Leeson had all four important assumptions for fraud:

- motivation – huge amount of money was at his disposal,
- knowledge – he possessed very well knowledge on processes in front and back offices,
- opportunity – he was manager controlling processes in both front and back offices; he was a key person in change management of business applications supporting the trading,
- access to assets – Leeson had access to financial assets through business applications.

External commercial audit was faulty. Until 1994 responsible commercial auditor was Deloitte & Touche. Leeson started with his fraudulent activities in 1992. After 1994, Coopers Leibrandt (nowadays known as PriceWaterhouse Coopers) audited Barings Bank but did not recover any anomalies in organization and control procedures.

So, external commercial audit did not fulfil their obligations adequately. When Barings officially declared pre tax profit of 100 million pounds Sterling, Leeson's account 88888 had 23 million pounds Sterling losses. External audit did not perceive that fact. Even worse negligence was repeated in next audit, when account 88888 totalled 208 million pounds Sterling.

On the other side, internal audit identified lack of control procedures, but after Singapore management dispute, internal audit excluded findings and recommendations from official report. Also, internal audit objections on inadequate segregation of duties were ignored by top management in London headquarters.

2.2 Analysis of Allied Irish Banks Case

Fraud committed by John Rusnak, employee of Allied Irish Bank (AIB) front office, was also based on use of computer software, inappropriate auditing processes and serious flaws in segregation of duties. Fraud resulted in 691 million USD of losses on 8th of February 2002.

Rusnak controlled and changed value at risk, the most important measure value used by AIB in order to monitor its forex exchange trades. He did that by directly changing the values in the spreadsheet calculation of the value at risk used by other employees in risk control unit. While employee in risk control unit was supposed to check the value at risk amounts, he relied on the content of Rusnak's Excel spreadsheet. Rusnak manipulated transaction values used for value at risk calculation. Just a straightforward control of comparing data in spreadsheet with other data sources would reveal the fraud.

Interestingly, occasionally since 1995 attention was given to a fact that prices of foreign exchange activities were not accessed and prepared independently of the employees performing the trades. Unfortunately, attempts to obtain independent prices were never completed.

In 2000, management of risk assessment unit responsible for foreign exchange activities expressed worries concerning the fact daily prices were obtained from spreadsheet created by traders. For some time, prices were printed from Reuter's information service and verified by risk control unit. Soon afterwards, risk control unit suggested that an Excel spreadsheet should be created which would download data from Reuter's service thus dismissing the necessity to manually check prices. It was agreed that on trustworthy front office employee should download trading data from Reuter's terminal to his personal computer and then append data to prepared Excel spreadsheet. That spreadsheet should be accessible by employees of front, back and middle offices. John Rusnak was nominated for that important task. From that moment on, all trading, reconciliation and control procedures performed in front, back and middle offices were based on data retrieved from before mentioned spreadsheet prepared by one trader.

The internal control employee soon noticed defective procedure and correctly commented that trader who prepared prices could have manipulated data. Recommendation was that back office should access foreign exchange pricing data independently of front office prepared spreadsheet. For this, one more licence of Reuter's service should have been bought and software installed. The bank should invest 10.000 USD. However, risk assessment management stated there is a constant need to cost cutting and that there is no necessity for duplication of work. Conclusion was data will be still prepared in front office and used as a data feed in back and middle offices.

Unfortunately, while objective was to save 10.000 USD, huge losses were recorded. No reconciliation or foreign exchange price checks were performed in back or middle offices.

Although after some time risk assessments analysts spotted that Rusnak's spreadsheet was altered and different from Reuter's data, no action was taken. It was discovered prices for yen and euro currencies, the two Rusnak performed the most trades, deviated significantly from Reuters.

Some six months after the risk assessment analyst revealed the prices spreadsheet was inconsistent with Reuter's data, only in April 2001, AIB remedied the issue. From that time on, both back and middle offices obtained independent copy of Reuter's service foreign exchange prices. However, losses were too significant, and in February 2002. AIB declared losses of 691 million USD caused by fraudulent foreign exchange trades.

2.3 Analysis of Riječka banka Case

Riječka banka was a third Croatian bank according to asset amount. In 2000, privatisation of bank occurred in accordance with international tender. The biggest shareholder and de facto owner of the bank became Bayerische Landesbank Girozentrale (BLB) from Munich with 59,9% of shares. Since then, bank continually undertook activities for rising market share.

Interestingly enough, bank earned ISO 9001 quality standard for all its business operations.

Auditing of banking activities was undertaken for various reasons. For purpose of privatisation, consultancy and legal advisory companies Deloitte Touche, HSBC and Norton Rose were involved in detailed checks and audit. Due diligence was performed in order to asses commercial, financial and legal situation in the bank. That activity ensured to potential buyers additional information about the bank.

Bank's financial reports were audited and verified by PriceWaterhouse Coopers (formerly Coopers Leibrandt) until 1999, and KPMG after year 2000. Internal audit department performed regular, special and subsequent audits.

Very first sign of problems in bank's trading activities on foreign markets appeared in March of 1999 when unknown individual notified Croatian National Bank (CNB) about some irregularities. CNB quickly responded by informing bank's board of management and insisted on explanation. Board of management replied to CNB that internal control procedures and monitoring of foreign trading transactions are in place and set in accordance to the best standards. Accordingly, front and back offices were segregated. Internal and commercial auditor did not notice any malfunction.

During 2000, CNB on-site supervision was accomplished in the areas of profit, capital, asset sources, liquidity, internal control and audit and bank's organization. Supervision concluded there were no significant irregularities.

However, in March of 2002 bank's board of management informs CNB on illegal activities related to transactions on foreign market that were revealed by internal audit department. It was assessed losses were between 83 and 103 million USD. KPMG, who audited the bank in 2001, withdrew its audit report. BLB notified CNB it would not recapitalize the bank

and so solve its losses. At the same time, private individuals and business entities started to withdraw their deposits.

CNB started with special on-site supervision in order to determine proportions of illegal activities and their influence on the bank's financial result.

Bank accepted formal internal procedures for each area of its business conduct. These procedures determined responsibilities and duties of employees together with strict procedures how processes must be carried out. Quality procedures were setup in accordance with ISO 9001 standard.

Therefore, operations including foreign market transactions were also covered by formal internal procedures. Specific and individual authorizations and restrictions were defined, permitted ways of transactions execution, rules concerning reporting of management etc. For each foreign market transaction type bank defined precise steps, documentation, responsibilities, duties and other procedural details. Separate formalized document confirmed who is responsible for conduct of certain transaction types. Also, it is defined what is maximum bank's exposure, what is maximum amount of single transactions and that all transactions must be closed on the opening day.

However, procedures were not conducted in accordance with formally accepted procedures and fraud was committed in rather simple way. Chief dealer managed to systematically avoid procedures and forge documentation in the course of several years. He tried to gain profit on foreign exchange market by inappropriate exposures and continually accumulated losses. Losses were not recorded in bank's accounting system, and were concealed in several ways:

- unauthorized borrowing from other banks
- booking of non-existence deposits in bank's assets
- contracting without final payments
- booking of transactions in incorrect currency or due dates

Chief dealer had opportunity to conceal his deeds because he carried out some activities that were beyond his authorization profile. At the same time, he traded on foreign markets, transferred funds by issuing payment messages, gave orders for booking in accounting system and even booked entries in accounting system. Also, it was noticed he very often stayed at work after the official working hours what was explained by having too much

work. After he stayed alone, he could perform activities without supervision and obstruction from other employees. Bank's advanced information system based on contemporary information technology solutions served as a very efficient means for contracting, transferring funds and phoney bookings. Some activities were performed under his own user account (operations in front office), but mostly under user accounts of his colleagues (operations in back office and accounting). He usually obtained usernames and passwords by social engineering techniques.

Disputes by other banks, resulting from overdue contracts, were regularly handled and resolved by chief dealer.

It is quite obvious that although procedures of conduct were defined and in accordance with best practices, control and audit activities were inadequate or even missing. Some of examinations that audit should have included are:

- checking if adequate measures of segregation of duties between employees of different business units exist so that there were no employees who can manipulate data in front office, back office and in accounting
- how reconciliation between front office and back office were done and who has the possibility to manipulate data
- checking if data transferred from back office to accounting department are accurate and trustworthy
- how employees authorize (login) to each information technology resource supporting business activity (SWIFT, Reuters, back office application, accounting application) and if all employees use their own authentication factors (passwords, smartcards, PINs)
- checking if adequate procedure of password management is established and whether it is followed by all employees;
- how application audit logs and audit trails are reviewed in order to check employees activities; reviews and check should have been done not only by management of foreign trade department but also by internal audit department, commercial audit and central bank's supervision

Additionally, it is obvious that fraud was based on data manipulation. If data analysis was adequately performed, possibly by use of information technology tools, fraud could have been prevented or at least significantly limited.

It was identified that total bank's losses in this case were 96,2 million USD.

Concerning the Riječka banka case, there were a few positive reactions and consequences drawn from the fraud and corresponding loss. First of all Croatian National Bank (CNB) and Government of Republic of Croatia reacted promptly, financially helped the bank what prevented bank's collapse and eventually possible domino effect. Individuals and business entities withdrawn some 350 million EUR from the Riječka banka but soon afterwards lot of clients returned. Also, thanks to stabilization activities performed by state officials, clients of other Croatian banks did not start to withdraw deposits. Furtherly, state authorities, institutions and agencies responsible for audit and supervision, as well as private entities started to pay attention to importance of information systems auditing. Understandably enough, leader in information systems auditing became Croatian National Bank.

2.4 Analysis of Societe Generale Case

Societe Generale, France's second biggest bank, almost went bankruptcy when the biggest trading losses in history was revealed in January 2008. The bank recognized losses were based on fraudulent moves by one of its junior traders named Jerome Kerviel. The amount of losses was 4,9 billion EUR.

However, Societe Generale has ranked first or second during the past five years in client surveys of equity derivative firms, according to Risk Magazine. In 2007, it received the award for "Equity Derivatives House of the Year" from The Banker, a London-based monthly magazine.

On 24th of January 2008, Societe Generale reported that rogue trader Jerome Kerviel bet on stock index futures of European markets hoping for profit but resulting in the biggest loss in history of banking and financial industry until discovery of fraud committed by Bernard Madoff in December 2008.

Generally speaking, future markets are the most popular daily trading markets and offer different markets such as stock index futures, currency futures and commodity futures. On all of these markets future contracts are traded. In future contracts it is specified that corresponding stock index, currency or commodity goods will be sold or bought at a

specific price on specific day in the future. Daily trading activity considers purchase of futures contracts in order to profit on the difference between buying and selling prices.

Stock index futures are markets where the commodity being traded is stock index, such as DAX (index of Deutche Boerse in Frankfurt) or Dow Jones (Chicago Board of Trade). So, trading with stock index futures does not involve trading with actual stocks (shares) but with certain calculated indices. Calculation of profit or loss is done on contract expiration date when underlying trading account is increased or decreased by the difference between actual price and price stated in futures contract.

Kerviel's futures trading came under interest for the first time on 18th of January 2008 when risk manager saw a single trade that was over limits set by the bank.

However, Societe Generale officials perceived rising problems on 21st of January 2008 when stock markets in France, United Kingdom and Germany recorded a drop of 5%. It was later discovered that Jerome Kerviel exceeded his trading limits and traded with 49.9 billion EUR, a value far greater than bank's capital. From 21st to 24th of January 2008, Societe Generale closed all opened (still not due) positions created by Kerviel which caused losses totalled at 4.9 billion EUR. Officials of Societe Generale described some of the means Kerviel used to evade bank's internally developed risk controls and detection. It is explained Kerviel was careful in closing the future trades after two or three days from purchase, just before the timed controls would cause notice would be sent from within application's internal control system to risk manager. Then, Kerviel would switch those values from older trades over to newly created trades. Some experts claimed that Kerviel's fraudulent scheme trades could have been unnoticed as a result of high volume of low risk transactions which were regularly and daily handled by trading division. Also, bank officials claimed that whenever control unit started to raise questions on some Kerviel's trades, he would interpret them as omission, Then he would cancel the corresponding transaction and replace it with another trade usually using a different instrument, dates and amounts to evade detection [33].

It is obvious that banks, despite the application of advanced risk management strategies, still can be under the threat that an employee with an understanding of its risk management processes can evade them and hide losses he caused. However, if auditing and data analysis were performed adequately, fraud could have been discovered much earlier.

2.5 Analysis of Madoff Case

In December 2008, as the financial crisis still devastated worldwide economies, a new financial scandal happened. Bernard Madoff, greatly praised investor and former chairman of the NASDAQ stock exchange, informed his sons that his asset management firm was based on a fraudulent scheme. Soon afterwards, their lawyers reported Bernard Madoff to federal authorities. Already on 11th of December 2008, Bernard Madoff was arrested and charged with financial fraud.

On 12th of March 2009, Madoff admitted guilty of crime he was charged for. It was soon revealed Madoff spoof his clients for 65 billion USD. Madoff claimed he was the only to blame for the fraud.

Madoff developed a widely known fraud system based on pyramidal structure. Pyramidal structure fraud is based on constantly growing pyramid base, i.e. the fact that more money is invested than paid out as capital gains. That is of course possible if the pyramid base is growing faster than the obligations for pay off. Simply said, previous investors having claims due were paid off of the deposits of newer investors. So, payments to investors were sourced from new investors' base and not from gains of investment itself. Such system is called Ponzi scheme, after Charles Ponzi, Italian immigrant to USA in the first half of 20th century, who created notorious pyramidal scheme based on post coupons.

Madoff system functioned well for years. However, due to deep financial crisis, some of his big customers requested to withdraw their investments. That finally caused knock down of a whole fraudulent scheme.

Although Madoff himself was described as a non-technical person, despising information technology, the use of information technology was at the core of the fraud. As it is explained in [1], the IBM server, an AS/400 that dated from the 1980s, was so old that some data had to be typed in by hand instead of automatic data download from different sources. Yet Madoff refused to replace it. It stored all data about fraudulent activities. The server, which has been audited by the government, was the nerve centre of the fraud. The thousands of pages of statements printed out from it showed trades that were never made.

After the arrest, Madoff disclosed he began with his pyramidal Ponzi scum in 1991. He claimed he had never invested any of his clients' assets ever since. Instead, he only

deposited the invested money on business account of his company in Chase Manhattan Bank. He was resolute to ensure high returns for his investors, despite financial crisis which started in 2008. Also, Madoff confessed he executed false trading transactions concealed by foreign money transfers and false reports toward SEC.

Some accused Securities and Exchange Commission (SEC) of being inactive and inefficient in recovering Madoff's fraud. The SEC had previously conducted several investigations into Madoff's business practices since 1999, however each finished with positive remarks for Madoff investment business. Some also criticized SEC for incompetence, use of inappropriate control and auditing methods together with sketchy approaches.

2.6 Conclusions on Causes

In chapters 2.1 through 2.5 it is shown how huge amounts of money can be lost or how bankruptcies were filed because of inappropriate control and auditing mechanisms. Significant component in mitigation of operational risks is adequate management of information systems. There are numerous standards, methodologies and approaches for development and maintenance of information systems. However, since information systems development and maintenance is usually extremely complex and interdisciplinary, their implementation and change management may be faulty. Faults may result in opportunities for fraud, omissions and errors. So, additional control and checks are indispensable in the form of information systems auditing. Unfortunately, although information systems control measures and auditing standards existed for years, they were not always applied adequately. Especially, data was not audited and controlled in appropriate way. That made possible such disastrous financial results shown previously.

Barings Bank bankruptcy was primarily outcome of:

- Inappropriate segregation of duty.
- Defects in data access rights settings which were result of inappropriate segregation of duty.
- Application development experts were under direct control of front and back offices manager.

- Inadequate control and auditing of business data and processes followed with non-existent computer assisted auditing of data and processes.
- Failure of change management procedures in development and maintenance of business applications.

In the case of Allied Irish Bank, Riječka banka and Societe Generale following omissions enabled the fraud:

- Inappropriate segregation of duty.
- Defects in data access rights settings which were result of inappropriate segregation of duty.
- Inadequate control and auditing of business data and processes followed with non-existent computer assisted auditing of data and processes.

In the Madoff case based on reasonably simple pyramidal fraud inadequate control and auditing of business data and processes followed with non-existent computer assisted auditing of data and processes caused the biggest scam in history of financial sector.

What can be learned from all these cases is the following:

- Information system and information technology can be used as a mean of execution and concealment of criminal activities.
- Process change management procedures, specifically change management of IT application supporting business process, should be appropriately implemented. For business critical processes, at least two lines of change authorizations are necessary;
- Segregation of duties in business processes is extremely important. Development and maintenance of IT solutions should be standardized, centralized and managed by lines of duty separated from those of business. Also, additional attention should be assigned to segregation of business functions. For all business functions, development of business applications must be centralized and segregated from business function which requests, uses and owns specific application.
- Information systems control and audit is mandatory. Specifically, auditing of data is indispensable. However, since data volumes may be extremely large, thus disabling manual work, computer assisted auditing tools are prerequisite for efficient and complete data audit. By use of computer assisted data audit, auditor may conclude if processes were fraudulent, result of errors or omissions.

What is clearly noticeable in all of cases explained previously, frauds were based on data manipulation. Fraudsters manipulated data in databases, operating transactions and reports based on operating transactions. Fraud schemes were so advanced that risk managers, internal and external, both commercial and state, auditors were convinced procedures were followed and no significant risks were noted. Also, in financial terms, all institutions which suffered enormous losses in previously shown examples were proclaimed extremely successful and profitable even very shortly before breakdown. That brings the conclusion that applied auditing methods were not appropriate. According to available information, auditors did not perform complete and careful data audit. If data were checked, it was done on a sample, usually prepared by auditee. That, of course, enabled the fraudsters to prepare arbitrary data and prevent auditors to find important issues. Data could not have been audited completely because auditors did not use computer assisted auditing methods nor tools. Computer based tools (computer assisted auditing tools - CAAT) with pre-defined auditing methods should have been applied. That way, auditors would have been concentrated primarily on business activity instead on development of functions for data analysis and auditing.

Additionally, obviously auditors performing the job were not skilful enough for such complex tasks of revealing fraud. That means that beside use of well designed computer assisted information system auditing methodology and CAAT, auditors have to improve their knowledge on business functions they audit, relations between function being audited and interfacing functions, knowledge on application systems supporting business, data structures and role of certain data in business processes.

3. Risks in Development and Use of Information Systems

3.1 Importance of Information Systems Management

There is considerable number of organizations in which information and information systems are the most valuable assets. Additionally, in contemporary competitive and constantly changing business environment, within the global crisis context which all economies are facing, management has increased expectations concerning quality of delivered information systems and information. Management requires additional quality, functionality and ease of use of information systems. It expects shorter delivery time and permanent improvement of services. At the same time, all mentioned above must be implemented at lower costs and with less personal/human resources.

Some organisations understand the potential of adequate implementation and use of new technology and information systems. However, successful organisations understand, manage and govern the risks associated with application and use of modern technology and information systems.

Since information are widely recognized as important business assets, business entities must provide quality, legal and security properties of their information, as for all other tangible or intangible assets. Management must also control and track optimisation of the use of available resources, including data within databases or flat files, application systems, hardware, technology and people - including users and IT development experts. In order to achieve adequate control and governance over its information system, management must clearly understand the status of its information system and agree what governance and security measures i.e. risk management controls they should implement.

3.2 Importance of Risk Based Approach

Contemporary business entities base their information systems on computer i.e. information technology. Information technology infrastructure and applications may be very complex, span different geographical locations, connect to public (unsecured) networks, allow direct communication with its customer base etc. With today's audit

approach, tools and auditor's expertise it is rarely possible to perform complete detailed audit of all subsystems and information systems components.

Consequence of such situation is the fact that auditor is confronted with the questions of what information system component to audit, when and how frequently. The only possible answer to this is to implement a risk-based approach.

There are numerous risk management methodologies which can be used in information systems risk assessment. However, risks of non-availability, non-integrity and non-confidentiality are in primary focus of all risk management methodologies and auditing approaches. It has to be born in mind that although these risks are implicit to information systems, these risks affect different systems in different ways and with different losses. For retail banking at a branch in city centre risk of non-availability even for an hour can be considerable. Consequent losses can be especially significant if banking market and competition are both developed and if mean time between failures that result in non-availability of retail banking function is shortened. The risk of non-integrity caused by unauthorized modification of data can be a source of frauds and potential losses. Unauthorized modification resulted from inappropriate access privileges was one of key issues that resulted in frauds explained in chapter 2. Potential intruder with more access rights that he should have is the major risk of fraud. This is especially true if person gained more access rights than it is needed through regular procedure of access rights assignment since it is not perceived as intrusion by eventual information system event monitoring system. Also, risk of non-confidentiality is particularly important since gaining confidential information by unauthorized persons can result in appearance of other risks - market, credit, reputation and even systemic.

Naturally, risk-based approach in auditing must begin with adequate risk assessment. After risk assessment is accomplished, audit plan must be defined. Audit plan must consist of all steps that should be performed by actual audit. It has to explain time frames of each activity, personally assigned responsibilities which are dependent of knowledge and experience of individual auditors, auditee obligations, information needed and ways of obtaining them, together with technical prerequisites.

The steps that should be followed for a risk-based approach in order to make an audit plan are:

1. Inventory the information systems in use in the organization and categorize them.
2. Determine which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate.
3. Assess what risks affect these systems and the severity of impact on the business.
4. Rank the systems based on the above assessment and decide the audit priority, resources, schedule and frequency [23, page 2].

The auditor can create an audit plan based on longer time frame that lists the separate audit assignments that will be scheduled, as well as the resources required.

Mapping of results of business risk assessment with information systems components is one of the keys to successful audit. Auditing must follow business risk assessment and focus on riskier information systems components. In order to create applicable audit plan auditor must clearly define personal skills and experience needed for specific audit as well as other resources and prerequisites.

After finishing audit plan it should be presented at the opening meeting with the senior management responsible for the information system area to be audited. It is possible that outcomes of that meeting will require one more round of amendments to audit plan. Such opening meeting gets management more involved and possibly clarifies previously questionable issues and misunderstandings. It helps audit in achieving smooth execution according to plan.

During the information systems audit, findings are often quite technical in its nature. Of course, it is obligatory to perform in depth technical information systems audit since information systems is largely dependent on information technology. So, information systems audit with no, or lacking, technical analysis is inadequate and insufficient. Similarly, without data analysis based on computer assisted audit techniques software, information systems auditing will lack very important dimensions of data accuracy, assessment of potential for fraud and even adequacy of business processes. Additionally, it is required that all findings in information systems audit are clearly matched to vulnerabilities in business processes. That way senior business management can easier understand risks in highly technical and often not enough understood information systems and related information technology and relate it to business cases.

3.3 Operational Risk and Basel II

Lately it was recognized that operational risks should be included into important risk control areas that certain entities, especially banks, should take into account when assess and manage risks. Operational risk management was put into focus of many banks by Basel II capital accord. The Bank for International Settlements body named Basel Committee on Banking Supervision proposed a new capital accord in 1999, which has come to be known as Basel II. Then followed extensive consultative period with the committee releasing additional proposals for consultation in January 2001 and April 2003. The committee also conducted three separate studies to estimate the quality of those proposals. The finalized Basel II accord was released in June 2004 [46].

Basel II is based on three pillars:

- Minimum capital requirements,
- Supervisory review and
- Market discipline.

Generally speaking, Basel II retains the definition of bank capital and the market risk provisions of the 1996 Amendment. It largely replaces the old treatment of credit risk, and it requires capital for operational risk.

Basel II capital accord mostly updates the previous treatment of credit risk, and it demands reservations of capital for operational risk. According to Basel II, operational risk is risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Although the operational risk can be applied to any business industry, this particular way of framing risk management is of particular relevance to the banking sector. Banking regulators, usually central banks and financial supervisory authorities, are responsible for establishing safeguards to protect against bankruptcy, insolvency, various problems in banking industry and specifically systemic failure of the banking system. Since operational risk contains significant risk for banks' functioning, it is defined how banks should define and which measures should be undertaken to mitigate that risk.

The following list contains the official Basel II defined loss event types that correspond to operational risk with some examples for each category [46, pages 224&225]:

1. Internal Fraud

Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party

Examples:

- Transactions not reported (intentional)
- Transaction type unauthorised (w/monetary loss)
- Mismarking of position (intentional)
- Fraud / credit fraud / worthless deposits
- Theft / extortion / embezzlement / robbery
- Misappropriation of assets
- Malicious destruction of assets
- Forgery
- Check kiting
- Smuggling
- Account take-over / impersonation / etc.
- Tax non-compliance / evasion (wilful)
- Bribes / kickbacks
- Insider trading (not on firm's account)

2. External Fraud

Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.

Examples:

- Theft/Robbery
- Forgery
- Check kiting
- Hacking damage
- Theft of information (w/monetary loss)

3. Employment Practices and Workplace Safety

Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events.

Examples:

- Compensation, benefit, termination issues
- Organised labour activity
- General liability
- Employee health & safety rules events
- Workers compensation
- Discrimination types

4. Clients, Products, & Business Practice

Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.

Examples:

- Fiduciary breaches / guideline violations
- Suitability / disclosure issues
- Retail customer disclosure violations
- Breach of privacy
- Aggressive sales
- Account churning
- Misuse of confidential information
- Lender liability
- Antitrust
- Improper trade / market practices
- Market manipulation
- Insider trading (on firm's account)
- Unlicensed activity
- Money laundering
- Product defects (unauthorised, etc.)
- Model errors
- Failure to investigate client per guidelines
- Exceeding client exposure limits
- Disputes over performance of advisory activities

5. Damage to Physical Assets

Losses arising from loss or damage to physical assets from natural disaster or other events.

Examples:

- Natural disaster losses
- Human losses from external sources (terrorism, vandalism)

6. Business Disruption & Systems Failures

Losses arising from disruption of business or system failures.

Examples:

- Hardware
- Software
- Telecommunications
- Utility outage / disruptions

7. Execution, Delivery, & Process Management

Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.

Examples:

- Miscommunication
- Data entry, maintenance or loading error
- Missed deadline or responsibility
- Model / system misoperation
- Accounting error / entity attribution error
- Other task misperformance
- Delivery failure
- Collateral management failure
- Reference Data Maintenance

Although all of these event types can influence proper execution of processes in information systems, internal fraud and execution, delivery and process management were most often of all operational risks cause of losses and even bankruptcies in banking industry in last decade. Management of operational risk is largely based on management of risks related with development and use of information systems and information technology.

More on Bank for International Settlement approach to operational risk subject can be found in chapter 4.2.

3.4 Operational Risk and FED

Federal Reserve System (FED) acts as a central banking authority of United States of America. The primary task of the FED is the creation of monetary policy which means it is bringing key decisions which influence the cost and availability of money in country economy. This also comprises discount rate policy, which together with open market operations constitute the monetary policy tools.

Beside its monetary policy tasks, FED also has regulatory and supervisory responsibilities over US banks, bank holding companies, international bank branches in the USA and foreign activities of member banks.

Furthermore, FED has a vital role in preserving the adequate functioning of the US payments system. FED also develops and maintains regulations related to consumer credits and consumer protection.

According to FED terminology [51], operational risk emerges from the possibility that inappropriate information systems, operational problems, flaws or failures in internal (especially information systems based) controls, fraud, or unexpected man made or natural disasters will result in unplanned losses. Effective governance of information systems optimizes the benefits from technology and assures achieving enterprise objectives. The departments responsible for development of information systems primarily typically manage IT operations, network and database administration, application systems development and acquisition of new technologies and solutions. Information systems governance should encompass all of previously mentioned areas plus managing providing expertise in choosing and operating technology solutions for an institution's lines of business such as (e.g. in banking) commercial credit and asset management, or enterprise-wide activities such as security, information systems project management, information systems change management, business continuity planning etc.. This dual role and the increasing use of technology raise the importance of IT governance in effective corporate governance.

Inadequate governance of information systems strategy, applications and infrastructure can result with out of step between business and information systems goals, as well as the inefficient use of information systems resources. Also, weaknesses in information systems

governance can produce additional weaknesses and even can create prerequisites for fraudulent activities. The result is highly increased operational risk. Some examples of inappropriate information systems governance are:

- Defect or lack of quality control and security mechanisms over information systems processes can result in incorrect data and information and reduce the credibility of information systems.
- Inappropriate or non existing business control mechanisms add risks to omissions, errors and fraudulent events.
- Defective or nonexistent information systems change management procedures may prevent implementation of adequate business needs and/or produce omissions, errors and frauds.
- Inadequate organizational structures can prevent the achievement of business goals.
- Unclear responsibilities and reporting lines can lead to defects in accountability and authority over business and information system processes [51].

Operational risk may be a result of fraud, omission or error. Fraud, omissions and errors are usually consequences of management's incompetence to manage data and information or to acquire products and services in appropriate manner can also inflict operational risk. Inappropriate management of operational risk may culminate in significant losses in information system including business obstructions or conduct of improper business activities. Banking institution is obliged to adequately determine, measure, oversee, and manage operational risk. Operational risk must be differentiated by management from other risk types with objective to assure permanent and consistent focus on mitigation of operational risk. The management's board must set up and approve special program for managing and monitoring of this risk type. That program should define what the bank's tolerance for risk is, the effectiveness of bank's controls, management's responsibility in relation to moderation of risk, and the necessary activities for effective management of information system. Operational risk management must include areas like application development and support, systems and infrastructure development and support, transaction management, customer service, internal controls, capacity planning and performance assurance. Operational risk from within information system also affects credit, compliance, strategic, reputation, and market risks:

- *Liquidity, interest, and price risks* – Credit and market risks can materialize from external changes in markets, industries, or specific customers. Internal controls that rely heavily on the availability and performance of technology

create additional operational risk exposure. For example, a failure to properly implement changes to underwriting, account management, or collection systems can lead to significant losses, and higher loan servicing and collection costs.

- *Reputation risk* – Reputation risk stems from errors, delays, or omissions in information technology that become public knowledge or directly affect business partners, customers and consumers resulting in a loss of confidential information and potential customer withdrawal of funds. Two activities that can lead to reputation risk are the unauthorized disclosure of confidential customer information and the hacking/modifying of an institution's website.
- *Strategic risk* – Strategic risk can stem from inaccurate information or analysis that causes management to make poor strategic decisions. For example, IT management could decide to save money by delaying an infrastructure upgrade to increase network bandwidth, which could result in a business line losing market share due to an inability to compete.
- *Compliance (legal) risk* – Compliance risk results from the institution's inability to meet the regulatory and legal requirements associated with its IT products and services. Legal risk may lead to civil or criminal liability if, for example, an institution discloses confidential information or provides inaccurate or untimely consumer compliance disclosures. [50]

Management of information system business function must have an integral and corporate-wide view of technology that supports information system. It must persist in maintenance of an active engagement in corporate planning with the aim of aligning information system and underlying technology with defined business objectives. Information system management also must provide that adequate controls exist throughout the bank. According to FED approach, management must assess risks and define how to manage and alleviate these risks. Management must permanently measure risk levels and compare them to results of business impact analysis. That is how management must continually redefine value of its business activities and prescribe acceptable risk levels.

4. Identification and Analysis of Existing Frameworks and Approaches for Information Systems Auditing

Frameworks and approaches to information systems auditing can be broadly divided into three groups:

1. Frameworks and approaches established and recommended by non-profit expert audit associations (e.g. Information Systems Audit and Control Association)
2. Approaches defined by industry specific associations and authorities (e.g. Bank for International Settlements)
3. Legally binding documents brought by country's authorities

There is no single approved and confirmed approach to information systems auditing, so there is no unique methodology that could be the one and only resource for information systems auditing planning, conduct and reporting. Probably unification is possible only on a high level definitions, scope and basic outlines of approach. However, unification on more detailed level will never be possible because each information system audited has its specifics, different risks, different business model and role of information system and corresponding information technology.

As it is shown in chapters 1 through 3, information systems are very important part of any business. Additionally, computer based components of information systems do not only store business transactions and data but enable critical business processes of the business entity. It is fully understandable that business management must have appropriate knowledge, control and also serious concerns about information systems status and development. The objective of information systems audit is to help management in better understanding of information system, risks, possibilities to mitigate risks, achieving alignment between business and information system, easier definition of priorities etc. Auditing process assures that by producing findings and giving recommendations.

Important issues that have to be covered by information systems auditing are:

1. Availability

It has to be answered on question if information system on which business is dependent will be available to business demands at all needed times? Is it reasonably protected against disasters or incidents?

2. Confidentiality

Reasonable measures have to be carried out in order to preserve non-disclosure of information to unauthorized persons.

3. Integrity

It must be ensured that information provided by the information system is always accurate, reliable and timely. All reasonable measures should be implemented in order to prevent unauthorized modifications to data, applications, hardware, networking equipment, system or other software.

After it is proved that risks in information systems have enormous impact on underlying business processes and functions, legal systems of considerable number of countries introduced necessity of information systems auditing. Procedures and approaches were usually overtaken from associations and good practice they supported (for example ISACA – Information Systems Audit and Control Association) but also from guidelines and requirements set by organizations influential in certain industries. The latter is especially applicable to banking industry and works of Bank for International Settlements (BIS), Federal Reserve System (FED) and International Monetary Fund (IMF). BIS, FED and IMF were for years instructing the banks and finance ministries about seriousness and significance of information systems auditing.

In the following chapters, methodologies and approaches accepted and announced by some of these prominent organizations are described in more details.

4.1 Approach of Information Systems Audit and Control Association

The most influential non-profit expert audit organization is Information Systems Audit and Control Association (ISACA). With more than 86.000 members in over 160 countries, ISACA is global leader in the field of IT auditing and control. ISACA began its activities in 1967, when a small group of individuals with similar jobs, auditing controls in the computer systems that were becoming increasingly critical to the operations of their organizations, sat down to discuss the need for a centralized source of information and guidance in the field. In 1969, the group formalized, incorporating as the EDP Auditors Association. In 1976 the association formed an education foundation to undertake large-scale research efforts to expand the knowledge and value of the IT governance and control

field [47]. ISACA developed globally applicable and accepted information systems auditing and control standards, guidelines and procedures.

ISACA sponsors international conferences, promotes the importance of IT auditing and control, administers the globally respected CISA (Certified Information Systems Auditor) professional title earned by more than 60.000 persons. CISA certificate is de facto worldwide standard and prerequisite for information systems auditing. It also established CISM (Certified Information Systems Manager) professional certificate which covers information security management domain of information systems.

Another of ISACA's strengths is its chapter network. ISACA has more than 175 chapters established in over 70 countries worldwide. Chapters ensure professional networking of its members and experts, education, upholding the necessity of information systems auditing and control and other benefits on a chapter's territory.

Furthermore, IT Governance Institute, established by the ISACA in 1998, brings original research, presentations at various conferences, and reports and documents created by experts in the area to assist management in their strive to make information systems successful in supporting the enterprise's objectives.

ISACA's vision and mission statements predicate that it exists to assist in IT governance, IT control, IT management, IT risks and IT process, and their interaction with corporate governance, corporate management, corporate risks and corporate processes. ISACA does that by providing value through various services, such as research, standards, information, education and certification. The Association helps IS audit, control and security professionals focus not only on IT, IT risks and security issues, but also on the relationship between IT and the business, business processes and business risks.

Croatian branch of ISACA (ISACA Croatian Chapter - ISACA CC) was founded in 2001, and already became a leader in IT auditing promotion and education in Croatia. ISACA CC is continuously working on raising the awareness among Croatian management concerning importance of IT auditing and security issues.

4.1.1 Information Systems Standards, Guidelines and Procedures for Auditing and Control Professionals

ISACA established documents which are de facto standards and have the widest use in information systems auditing in the world. The document of primary interest for auditors and auditing practice is "IS Standards, Guidelines and Procedures for Auditing and Control Professionals". That document is a framework for the information systems auditing ensuring a few levels of expertise.

Standards section defines obligatory and minimum requisites for information systems auditing. Standards set the necessary amount and quality of work done by information systems auditors in order to fulfil professional responsibilities as set in ISACA Code of Professional Ethics for Information Systems Auditors. Their intention is also to prove to management that auditors who comply with Standards, Guidelines and Procedures are performing auditing work according to best existing practices. Standards also set requirements for CISA (Certified Information Systems Auditor) professional designation. Those who are not following Standards are subject to investigation and discipline actions up to suspension of CISA certificate.

Currently, there are 16 standards available:

S1 Audit Charter
S2 Independence
S3 Professional Ethics and Standards
S4 Competence
S5 Planning
S6 Performance of Audit Work
S7 Reporting
S8 Follow-Up Activities
S9 Irregularities and Illegal Acts
S10 IT Governance
S11 Use of Risk Assessment in Audit Planning
S12 Audit Materiality
S13 Using the Work of Other Experts
S14 Audit Evidence
S15 IT Controls

S16 E-commerce

Currently there are two standards under development: continuous audit and computer assisted audit techniques.

Guidelines section ensures instructions how to implement Information Systems Auditing Standards. Auditor should consider guidelines in order to set out how to apply standards. Primary aim of the IS Auditing Guidelines is to ensure additional information how auditing should be performed in order to be compliant with the IS Auditing Standards. Currently there are 39 guidelines:

G1 Using the Work of Other Auditors
G2 Audit Evidence Requirement
G3 Use of Computer Assisted Audit Techniques (CAATs)
G4 Outsourcing of IS Activities to Other Organisations
G5 Audit Charter
G6 Materiality Concepts for Auditing Information Systems
G7 Due Professional Care
G8 Audit Documentation
G9 Audit Considerations for Irregularities and Illegal Acts
G10 Audit Sampling
G11 Effect of Pervasive IS Controls
G12 Organisational Relationship and Independence
G13 Use of Risk Assessment in Audit Planning
G14 Application Systems Review
G15 Planning
G16 Effect of Third Parties on an Organisation's IT Controls
G17 Effect of Nonaudit Role on the IS Auditor's Independence
G18 IT Governance
G20 Reporting
G21 Enterprise Resource Planning (ERP) Systems Review
G22 Business-to-consumer (B2C) E-commerce Review
G23 System Development Life Cycle (SDLC) Review
G24 Internet Banking
G25 Review of Virtual Private Networks

G26 Business Process Reengineering (BPR) Project Reviews
G27 Mobile Computing
G28 Computer Forensics
G29 Post-implementation Review
G30 Competence
G31 Privacy
G32 Business Continuity Plan (BCP) Review From It Perspective
G33 General Considerations on the Use of the Internet
G34 Responsibility, Authority and Accountability
G35 Follow-up Activities
G36 Biometric Controls
G37 Configuration Management Process
G38 Access Controls
G39 IT Organisation
G40 Review of Security Management Practices

There are three guidelines still in development stage: enterprise security architecture, project management methodology and return on security investment (ROSI).

Procedures contain examples of detailed steps that auditor can undertake during auditing assignments. The procedures ensure information on how to closely follow the standards when performing the information systems auditing tasks. Currently, there are 12 procedures:

P1 IS Risk Assessment
P2 Digital Signatures
P3 Intrusion Detection
P4 Viruses and other Malicious Code
P5 Control Risk Self-assessment
P6 Firewalls
P7 Irregularities and Illegal Acts
P8 Security Assessment—Penetration Testing and Vulnerability Analysis
P9 Evaluation of Management Controls Over Encryption Methodologies
P10 Business Application Change Control
P11 Electronic Funds Transfer (EFT)

These three groups of documents (standards, guidelines and procedures) provide auditors with indispensable material for adequate practical information systems auditing. Documents thoroughly cover all areas of information systems audit and give clear explanations in both standards and guidelines sections with practical examples how audit should be performed in actual information technology environments within procedures section. Materials are under constant review especially guidelines and procedures sections which are by their more practical nature subject to more frequent changes.

Before mentioned guideline "G3 Use of Computer Assisted Audit Techniques (CAATs)" explains the importance of computer assisted auditing tools and techniques, gives broad overview of CAATs use in audit planning, audit execution, audit documentation and reporting. However, this guideline does include definition of computer assisted information systems auditing methodology nor gives any recommendation on which methods should be used and when. Such broad approach leaves auditor with a number of choices resulting in varying and inconsistent audits performed by different (or even the same) auditors on different (or even the same) data sets. Although guideline G3 gives certain recommendations, especially concerning risks of using CAATs, CAATs planning steps, importance of arrangements with auditee and risks in gathering of audit evidence it certainly lacks more details in the field of audit execution, definition of methods and adequate computer assisted information systems auditing methodology.

4.1.2 Control Objectives for Information and Related Technologies (COBIT)

It is indispensable that business management has understanding of the risks and obstacles information systems and underlying information technologies are facing in order to ensure adequate direction of further development and proper management controls. COBIT, created and maintained by ISACA, is de facto standard methodology for binding business risks, management control and information technology areas. COBIT assures

- control system to manage business requirements for confidentiality, integrity, availability, compliance and reliability of information.
- that due diligence is exercised by all individuals involved in the management, use, design, development, maintenance or operation of information systems.
- development of understandable and clear policy and good practice for control of information systems. [40]

Business entities must ensure quality and security requirements for their data and information, as for all other important assets. Management must carry out reasonable activities to optimise the use of resources, including data and information, business applications, technical infrastructure, facilities and personnel.

COBIT is developed to be used not only as guidance for management and process owners, but also as a tool for information systems auditors. It sets clear definition of all indispensable information systems processes that usually exist in any business entity. Information systems audits can be carried out using process definition and recommendations for their optimization set in COBIT.

COBIT sets out from a postulate that: information system resources must be managed and controlled by processes grouped in certain way in order to ensure the information that business needs to fulfil its objectives. COBIT consists of a 34 high-level control objectives grouped into four broad domains: planning and organisation, acquisition and implementation, delivery and support, and monitoring and evaluation. Each of these objectives can be matched with the information systems processes. The business process owner can assure management that an adequate control system is set in information system by putting in practice these 34 high-level control objectives.

Briefly, the COBIT products include:

- Board Briefing on IT Governance - Helps executives understand why IT governance is important, what its issues are and what their responsibility is for managing it
- Management guidelines/maturity models - Help assign responsibility, measure performance, and benchmark and address gaps in capability
- Frameworks - Organise IT governance objectives and good practices by IT domains and processes, and links them to business requirements
- Control objectives - provide a complete set of high-level requirements to be considered by management for effective control of each IT process
- IT Governance Implementation Guide: Using COBIT and Val IT TM - provides a generic road map for implementing IT governance using the COBIT and Val ITEM resources

- COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance - Provides guidance on why controls are worth implementing and how to implement them
- IT Assurance Guide: Using COBIT - Provides guidance on how COBIT can be used to support a variety of assurance activities together with suggested testing steps for all the IT processes and control objectives [42]

Plan and Organize Domain

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. The realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. A proper organisation as well as technological infrastructure should be put in place. This domain typically addresses the following management questions [42]:

- Are IT and the business strategy aligned?
- Is the enterprise achieving optimum use of its resources?
- Does everyone in the organisation understand the IT objectives?
- Are IT risks understood and being managed?
- Is the quality of IT systems appropriate for business needs?

Processes in this domain are:

PO1 Define a Strategic IT Plan and direction
PO2 Define the Information Architecture
PO3 Determine Technological Direction
PO4 Define the IT Processes, Organization and Relationships
PO5 Manage the IT Investment
PO6 Communicate Management Aims and Direction
PO7 Manage IT Human Resources
PO8 Manage Quality
PO9 Assess and Manage IT Risks
PO10 Manage Projects

Acquire and Implement Domain

To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and

maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives. This domain typically addresses the following management questions [42]:

- Are new projects likely to deliver solutions that meet business needs?
- Are new projects likely to be delivered on time and within budget?
- Will the new systems work properly when implemented?
- Will changes be made without upsetting current business operations?

This domain contains of following processes:

AI1 Identify Automated Solutions
AI2 Acquire and Maintain Application Software
AI3 Acquire and Maintain Technology Infrastructure
AI4 Enable Operation and Use
AI5 Procure IT Resources
AI6 Manage Changes
AI7 Install and Accredit Solutions and Changes

Deliver and Support Domain

This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and operational facilities. It typically addresses the following management questions [42]:

- Are IT services being delivered in line with business priorities?
- Are IT costs optimised?
- Is the workforce able to use the IT systems productively and safely?
- Are adequate confidentiality, integrity and availability in place for information security?

Deliver and Support domain has following processes:

DS1 Define and Manage Service Levels
DS2 Manage Third-party Services
DS3 Manage Performance and Capacity
DS4 Ensure Continuous Service
DS5 Ensure Systems Security

DS6 Identify and Allocate Costs
DS7 Educate and Train Users
DS8 Manage Service Desk and Incidents
DS9 Manage the Configuration
DS10 Manage Problems
DS11 Manage Data
DS12 Manage the Physical Environment
DS13 Manage Operations

Monitor and Evaluate Domain

All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance and governance. It typically addresses the following management questions [42]:

- Is IT's performance measured to detect problems before it is too late?
- Does management ensure that internal controls are effective and efficient?
- Can IT performance be linked back to business goals?
- Are adequate confidentiality, integrity and availability controls in place for information security?

Monitor and Evaluate domain includes following processes:

ME1 Monitor and Evaluate IT Processes
ME2 Monitor and Evaluate Internal Control
ME3 Ensure Regulatory Compliance
ME4 Provide IT Governance

As it is noted above, across four domains, COBIT has identified 34 IT processes that are generally used.

While most enterprises have defined plan, build, run and monitor responsibilities for IT, and most have the same key processes, few will have the same process structure or apply all 34 COBIT processes. COBIT provides a complete list of processes that can be used to verify the completeness of activities and responsibilities; however, they need not all apply, and, even more, they can be combined as required by each enterprise [42, page 13].

In addition, corresponding to each of the 34 high-level control objectives is an audit guideline to enable the review of IT processes against COBIT's 318 recommended detailed control objectives to provide management assurance and/or advice for improvement. The guidelines are action oriented and generic and provide management direction for getting the enterprise's information and related processes under control, for monitoring achievement of organisational goals, for monitoring performance within each IT process and for benchmarking organisational achievement. To achieve desired goals and objectives management and auditors must constantly and consistently re-check procedures. Audit Guidelines outlines and suggests actual activities to be performed corresponding to each of the 34 high-level IT control objectives, while substantiating the risk of control objectives not being met. It assists in analysing an organisation's IT control environment to substantiate their opinions and/or provide advice to management on internal controls [41, page 1].

ISACA also provides lessons learned from those organisations that successfully applied COBIT in their work environments through its implementation guidelines.

4.2 Bank for International Settlements Approach

The Bank for International Settlements (BIS) is an international organisation which fosters international monetary and financial cooperation and serves as a bank for central banks.
The BIS fulfils this mandate by acting as:

- a forum to promote discussion and policy analysis among central banks and within the international financial community
- a centre for economic and monetary research
- a prime counterparty for central banks in their financial transactions
- agent or trustee in connection with international financial operations [37]

The Bank's head office is in Basel, Switzerland. There are also two representative or branch offices: in the Hong Kong Special Administrative Region of the People's Republic of China and in Mexico City. The BIS was established in 1930, which makes the BIS the world's oldest international financial organisation. As its customers are central banks and international organisations, the BIS does not accept deposits from, or provide financial services to private individuals or corporate entities. [37]

The BIS is a leading organization in risk management in banking industry. For decades it deals with and defines procedures for mitigation of credit, market and reputation risk. Although, in last decade it strongly focuses on operational risk management.

The BIS strongly believes that certain rules must be implemented for the management of operational risk, as it is already done for decades for the management of other significant risks. The lacking management of operational risk can result in a fault statement of bank's risk-return on investment rate and expose it to significant losses. Risk of inappropriate development, use and maintenance of information systems is understood as one of key operational risks.

One of very important tasks of BIS is setting sound banking supervision policies. Banking supervision consists of a number of control measures and procedures:

- regulation of bank's entry into market, conduct of business, going out of business
- identification of owner's responsibilities for bank's conduct of business,
- control of bank's risk management activities
- consolidated banking oversight,
- consumer's protection,
- cooperation with other supervisory and auditing institutions (foreign and domestic)

From this definition it is visible that supervision is much more than auditing which is more focused on review of internal risks, procedures and finding of possible fraudulent activities.

In order to establish proper controls of information systems risks, a framework should be established with objective to install adequate auditing function within a bank. A bank should develop a framework for managing operational risk and evaluate the adequacy of capital concerning its operational risk. The framework should cover the bank's appetite and tolerance for operational risk, as specified through the policies for managing this risk, including the extent and manner in which operational risk is transferred outside the bank. It should also include policies outlining the bank's approach to identifying, assessing, monitoring and controlling/mitigating the risk. [46]

BIS issued "Core Principles for Effective Banking Supervision" where basic guidelines are set for banking supervision by financial authorities. The Core Principles are a framework

of minimum standards for sound supervisory practices and are considered universally applicable. The BIS drew up the Core Principles and the Methodology as its contribution to strengthening the global financial system. Weaknesses in the banking system of a country, whether developing or developed, can threaten financial stability both within that country and internationally. The Committee believes that implementation of the Core Principles by all countries would be a significant step towards improving financial stability domestically and internationally and provide a good basis for further development of effective supervisory systems [43, page 2].

The document very briefly covered area of operational risk management (Principle 15): ”Supervisors must be satisfied that banks have in place risk management policies and processes to identify, assess, monitor and control/mitigate operational risk. These policies and processes should be commensurate with the size and complexity of the bank.” [43, page 4]. Also, the document touched the desirable characteristics of supervisory approach, techniques and reporting in principles 19, 20 and 21:
“Principle 19 – Supervisory approach: An effective banking supervisory system requires that supervisors develop and maintain a thorough understanding of the operations of individual banks and banking groups, and also of the banking system as a whole, focusing on safety and soundness, and the stability of the banking system.

Principle 20 – Supervisory techniques: An effective banking supervisory system should consist of on-site and off-site supervision and regular contacts with bank management.

Principle 21 – Supervisory reporting: Supervisors must have a means of collecting, reviewing and analysing prudential reports and statistical returns from banks on both a solo and a consolidated basis, and a means of independent verification of these reports, through either on-site examinations or use of external experts.” [43, pages 4&5].

In October 2003, the BIS issued paper “Sound Practices for the Management and Supervision of Operational Risk”. The paper consists of the following chapters:

- developing an appropriate risk management environment;
- risk management: identification, assessment, monitoring and control/mitigation;
- the role of supervisors;
- the role of disclosure.

It is clear that operational risk differs from other banking risks. Typically it is not directly taken in return for an expected reward, but exists in the normal course of corporate activity which affects the risk management process. At the same time, failure to properly manage operational risk can result in a misstatement of an institution's risk profile and expose the institution to significant losses. Reflecting the different nature of operational risk, BIS defines a term "management" of operational risk as identification, assessment, monitoring and control or mitigation of risk.

a) developing an appropriate risk management environment

The board of directors should ensure that the bank's operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.

Both the board and senior management are responsible for creating an organisational culture that places high priority on effective operational risk management and adherence to sound operating controls.

An operational risk framework should be based on an appropriate definition of operational risk which clearly articulates what constitutes operational risk in that bank. The framework should cover the bank's appetite and tolerance for operational risk, as specified through the policies for managing this risk and the bank's prioritisation of operational risk management activities, including the extent of, and manner in which, operational risk is transferred outside the bank.

Since a significant aspect of managing operational risk relates to the establishment of strong internal controls, it is particularly important that the board establishes clear lines of management responsibility, accountability and reporting. In addition, there should be separation of responsibilities and reporting lines between operational risk control functions, business lines and support functions in order to avoid conflicts of interest.

Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank's material products, activities, processes and systems. Banks should have in place adequate internal audit coverage to verify that operating

policies and procedures have been implemented effectively. The board should ensure that the scope and frequency of the audit programme is appropriate to the risk exposures. Audit should periodically validate that the firm's operational risk management framework is being implemented effectively across the firm. To the extent that the audit function is involved in oversight of the operational risk management framework, the board should ensure that the independence of the audit function is maintained. This independence may be compromised if the audit function is directly involved in the operational risk management process. The audit function may provide valuable input to those responsible for operational risk management, but should not itself have direct operational risk management responsibilities. In practice, the Committee recognises that the audit function at some banks (particularly smaller banks) may have initial responsibility for developing an operational risk management programme. Where this is the case, banks should see that responsibility for day-to-day operational risk management is transferred elsewhere in a timely manner [54, pages 6-7].

b) risk management: identification, assessment, monitoring and control/mitigation

Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures. Risk identification is paramount for the subsequent development of a viable operational risk monitoring and control system. Effective risk identification considers both internal factors (such as the bank's structure, the nature of the bank's activities, the quality of the bank's human resources, organisational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of the bank's objectives.

In addition to identifying the most potentially adverse risks, banks should assess their vulnerability to these risks. Effective risk assessment allows the bank to better understand its risk profile and most effectively target risk management resources. Risk indicators must be thoroughly analysed. They are statistics and/or metrics, often financial, which can provide insight into a bank's risk position. Indicators must be reviewed on a periodic basis (such as monthly or quarterly) to alert banks to changes that may be indicative of risk

concerns. Such indicators may include the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions.

Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk. In addition to monitoring operational loss events, banks should identify appropriate indicators that provide early warning of an increased risk of future losses. Such indicators (often referred to as key risk indicators or early warning indicators) should be forward-looking and could reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, transaction breaks, system downtime, and so on. When thresholds are directly linked to these indicators an effective monitoring process can help identify key material risks in a transparent manner and enable the bank to act upon these risks appropriately.

In addition to segregation of duties, banks should ensure that other internal practices are in place as appropriate to control operational risk. Examples of these include:

- close monitoring of adherence to assigned risk limits or thresholds;
- maintaining safeguards for access to, and use of, bank assets and records;
- ensuring that staff have appropriate expertise and training;
- identifying business lines or products where returns appear to be out of line with reasonable expectations (e.g., where a supposedly low risk, low margin trading activity generates high returns that could call into question whether such returns have been achieved as a result of an internal control breach);
- regular verification and reconciliation of transactions and accounts,
- checking for compliance with management controls;
- policies, processes and procedures concerning the review, treatment and resolution of non-compliance issues; and
- a system of documented approvals and authorisations to ensure accountability to an appropriate level of personnel

Failure to implement such practices has resulted in significant losses for some banks in recent years.

Operational risk can be more pronounced where banks engage in new activities or develop new products (particularly where these activities or products are not consistent with the bank's core business strategies), enter unfamiliar markets, and/or engage in businesses that are geographically distant from the head office. Moreover, in many such instances, firms do not ensure that the risk management control infrastructure keeps pace with the growth in the business activity. A number of the most sizeable and highest-profile losses in recent years have taken place where one or more of these conditions existed. Therefore, it is incumbent upon banks to ensure that special attention is paid to internal control activities where such conditions exist. Some significant operational risks have low probabilities but potentially very large financial impact. Moreover, not all risk events can be controlled (e.g., natural disasters). Risk mitigation tools or programs can be used to reduce the exposure to, or frequency and/or severity of, such events. For example, insurance policies, particularly those with prompt and certain pay-out features, can be used to externalize the risk of "low frequency, high severity" losses which may occur as a result of events such as third-party claims resulting from errors and omissions, physical loss of securities, employee or third-party fraud, and natural disasters.

Investments in appropriate processing technology and information technology security are also important for risk mitigation. However, banks should be aware that increased automation could transform high-frequency, low-severity losses into low frequency, high-severity losses. The latter may be associated with loss or extended disruption of services caused by internal factors or by factors beyond the bank's immediate control (e.g., external events). Such problems may cause serious difficulties for banks and could jeopardise an institution's ability to conduct key business activities.

Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption. Banks should identify critical business processes, including those where there is dependence on external vendors or other third parties, for which rapid resumption of service would be most essential. For these processes, banks should identify alternative mechanisms for resuming service in the event of an outage. Particular attention should be paid to the ability to restore electronic or physical records that are necessary for business resumption. Where such records are backed-up at an off-site facility, or where a bank's operations must be relocated to a new site, care should be taken that these sites are at an

adequate distance from the impacted operations to minimise the risk that both primary and back-up records and facilities will be unavailable simultaneously. [54, pages 8-12]

c) Role of Supervisors

Since one of most important roles of the BIS is giving guidelines how state supervision should be performed, crucial part of this paper covers the question of supervisors. Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks as part of an overall approach to risk management.

Supervisors should require banks to develop operational risk management frameworks consistent with the guidance in this paper and commensurate with their size, complexity, and risk profiles. To the extent that operational risks pose a threat to banks' safety and soundness, supervisors have a responsibility to encourage banks to develop and use better techniques in managing those risks.

Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank's policies, procedures and practices related to operational risks. Supervisors should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at banks.

Examples of what an independent evaluation of operational risk by supervisors should review include the following:

- The effectiveness of the bank's risk management process and overall control environment with respect to operational risk;
- The bank's methods for monitoring and reporting its operational risk profile, including data on operational losses and other indicators of potential operational risk;
- The bank's procedures for the timely and effective resolution of operational risk events and vulnerabilities;
- The bank's process of internal controls, reviews and audit to ensure the integrity of the overall operational risk management process;
- The effectiveness of the bank's operational risk mitigation efforts, such as the use of insurance;
- The quality and comprehensiveness of the bank's disaster recovery and business continuity plans; and

- The bank’s process for assessing overall capital adequacy for operational risk in relation to its risk profile and, if appropriate, its internal capital targets.

Supervisors should also seek to ensure that, where banks are part of a financial group, there are procedures in place to ensure that operational risk is managed in an appropriate and integrated manner across the group. In performing this assessment, cooperation and exchange of information with other supervisors, in accordance with established procedures, may be necessary. Some supervisors may choose to use external auditors in these assessment processes.

Deficiencies identified during the supervisory review may be addressed through a range of actions. Supervisors should use the tools most suited to the particular circumstances of the bank and its operating environment. In order that supervisors receive current information on operational risk, they may wish to establish reporting mechanisms, directly with banks and external auditors (for example, internal bank management reports on operational risk could be made routinely available to supervisors).

Given the general recognition that comprehensive operational risk management processes are still in development at many banks, supervisors should take an active role in encouraging ongoing internal development efforts by monitoring and evaluating a bank’s recent improvements and plans for prospective developments. These efforts can then be compared with those of other banks to provide the bank with useful feedback on the status of its own work. Further, to the extent that there are identified reasons why certain development efforts have proven ineffective, such information could be provided in general terms to assist in the planning process. In addition, supervisors should focus on the extent to which a bank has integrated the operational risk management process throughout its organisation to ensure effective business line management of operational risk, to provide clear lines of communication and responsibility, and to encourage active self assessment of existing practices and consideration of possible risk mitigation enhancements. [54, pages 13-14]

d) Role of Disclosure

Banks should make sufficient public disclosure to allow market participants to assess their approach to operational risk management. The BIS believes that the timely and frequent public disclosure of relevant information by banks can lead to enhanced market discipline

and, therefore, more effective risk management. The amount of disclosure should be commensurate with the size, risk profile and complexity of a bank's operations. The BIS believes that a bank should disclose its operational risk management framework in a manner that will allow investors and counterparties to determine whether a bank effectively identifies, assesses, monitors and controls/mitigates operational risk [54, page 14].

4.3 Federal Reserves Bank (FED) Approach

Since one of key roles of Federal Reserves Bank are banking supervisory and auditing activities, it issued a number of guidances and obligatory requirements banks should fulfil in order to be compliant with FED requirements. A key document covering a subject of information systems auditing issued by FED is "Audit - IT Examination Handbook". This document provides guidance to supervisors, auditors and financial institutions on the characteristics of an appropriate information system and technology audit function.

One of key FED prerequisites of establishment of appropriate auditing procedure is definition of planned and structured audit program. It is essential that audit function has responsibility, knowledge and support of bank's board in evaluating bank's risk management practices, compliance with corporate policies concerning IT-related risks, internal control systems. This is a minimum set of tasks that must be preserved at bank of any size and complexity. Effective audit functions are risk-based, promote reliable IT controls, ensure quick solution to deviations and report the board of the suitability of implemented risk management practices and measures.

FED understands that effective IT audit should:

- Identify areas of greatest IT risk exposure to the institution in order to focus audit resources.
- Promote the confidentiality, integrity, and availability of information systems.
- Determine the effectiveness of management's planning and oversight of IT activities.
- Evaluate the adequacy of operating processes and internal controls.
- Determine the adequacy of enterprise-wide compliance efforts related to IT policies and internal control procedures.

- Require appropriate corrective action to address deficient internal controls and follow up to ensure management promptly and effectively implements the required actions. [38, page 2].

The board of directors and senior management are responsible for ensuring that the institution's system of internal controls operates effectively. One important element of an effective internal control system is an internal audit function that includes adequate IT coverage.

To meet its responsibility of providing an independent audit function with sufficient resources to ensure adequate IT coverage, the board of directors or its audit committee should

- Provide an internal audit function capable of evaluating IT controls,
- Engage outside consultants or auditors to perform the internal audit function, or
- Use a combination of both methods to ensure that the institution has received adequate IT audit coverage.

An institution's board of directors may establish an "audit committee" to oversee audit functions and to report on audit matters periodically to the full board of directors. For purposes of this booklet, the term "audit committee" means the committee with audit oversight regardless of the type of financial institution.4 Audit committee members should have a clear understanding of the importance and necessity of an independent audit function.

To comply with the Sarbanes-Oxley Act of 2002, public stock-issuing institutions are required to appoint outside directors as audit committee members. All members of a stock-issuing institution's audit committee must be members of the board of directors and be independent (i.e., not otherwise compensated by, or affiliated with, the institution). Additionally, Federal Deposit Insurance Corporation Improvement Act (FDICIA) requires all depository institutions with total assets greater than $500 million to have independent audit committees. Although not all institutions are subject to these requirements due to their corporate structure (Sarbanes-Oxley) or their size (FDICIA), it is generally considered good practice that they use them as guidelines to ensure the independence of their audit committees.

The board of directors should ensure that written guidelines for conducting IT audits have been adopted. The board of directors or its audit committee should assign responsibility for the internal audit function to a member of management (hereafter referred to as the "internal audit manager") who has sufficient audit expertise and is independent of the operations of the business.

The board should carefully review the placement of the audit function in relation to the bank's management structure. The board should have confidence that the internal audit staff members will perform their duties with impartiality and not be unduly influenced by senior management and managers of day-to-day operations. Accordingly, the internal audit manager should report directly to the board of directors or its audit committee.

The bank's board must understand existence of significant risks and appropriately undertaken control procedures including risks in new information system products, components and procedures. Board and operational management in all business functions must clearly understand that a number of risks are associated with reliance on technology, such as:

- Inappropriate user access to information systems
- Unauthorized disclosure of confidential information
- Unreliable or costly implementation of IT solutions
- Inadequate alignment between IT systems and business objectives
- Inadequate systems for monitoring information processing and transactions
- Ineffective training programs for employees and system users
- Insufficient due diligence in IT vendor selection
- Inadequate segregation of duties
- Incomplete or inadequate audit trails
- Lack of standards and controls for end-user systems
- Ineffective or inadequate business continuity plans
- Financial losses and loss of reputation related to systems outages.

The board or its audit committee members should seek training to fill any gaps in their knowledge related to IT risks and controls. The board of directors or its audit committee should periodically meet with both internal and external auditors to discuss audit work performed and conclusions reached on IT systems and controls [38, pages 3-5].

In each bank, independently of its size, capital or liabilities, effective risk-based audit function must be instituted. Risk-based audit function must encompass all institution's core and critical processes. The order, frequency and depth of particular business process' audit will differentiate according to the risk assessment results for certain business process.

Risk-based IT audit must:

- Identify the institution's data, application and operating systems, technology, facilities, and personnel;
- Identify the business activities and processes within each of those categories;
- Include profiles of significant business units, departments, and product lines, or systems, and their associated business risks and control features, resulting in a document describing the structure of risk and controls throughout the institution;
- Use a measurement or scoring system that ranks and evaluates business and control risks for significant business units, departments, and products;
- Include board or audit committee approval of risk assessments and annual risk-based audit plans that establish audit schedules, audit cycles, work program scope, and resource allocation for each area audited;
- Implement the audit plan through planning, execution, reporting, and follow-up;
- Include a process that regularly monitors the risk assessment and updates it at least annually for all significant business units, departments, and products or systems. [38, page 15&16]

Special care should be given to development, acquisition, or conversion of business applications since they are one of basis for performing banking activities. Also, through business applications it is possible to gain enormous advantage comparing to competition, but also, if controls are lacking, huge losses and even bankruptcies may occur. Some examples of such outcomes are shown in chapter 2. Application development is a complex process which demands intensive interaction between IT department, business departments, and internal audit. It necessitates set up of exact steps to ensure that applications satisfy business requirements. The auditor should check if requirements are met after each development step. He must check if testing was performed according to

sound practices and established procedures and whether application controls are set on input, processing, output and store level. Also, audit trails must be established for key user and application activities. Audit function must form instructions how to check applications in their analysis and design phase. It is necessary because implementation of control structures into application which is already in production environment is usually extremely uncomfortable.

After new application or critical change in existing application is approved and installed in production environment, auditors must carry out so-called post implementation check. This check must comprise of detailed testing of input controls, authentication mechanism, granted privileges, application algorithms, error handling, auditing of user and automated application activities and output results. This kind of test confirms not only if application operates as it is defined by user specification, but also checks if there are any flaws, mistakes or omissions in user specification that could not be found during previously performed testing and audit checks. This is possible since data available in testing environment in complex systems can be imperfect. Swift post implementation application audit will eliminate or at least minimize possible financial losses from application inefficiency, errors or missing controls. Also, reputation risk of incomplete or inaccurate information given to third parties or customers should be mitigated.

It is very important to stress that FED was among first supervisory and auditing institutions which realized importance and necessity of reliance on computer assisted auditing methods and supporting software in examination of information systems. After FED's initiative, number of other commercial audit companies which used CAAT's started to grow considerably. FED demands that CAATs have to be used to enhance audit findings and recommendations. It is very important that by use of CAATs cost of data, internal logic and audit of procedures can be significantly reduced. The use of CAATs may include audit software, business data, trace functions in application development environments, audit trails analyzers and security information and event management systems.

As a conclusion, FED insists that specific audit programme must be undertaken in following areas:

- The adequacy of management's involvement in risk management functions and audit
- Systems development and acquisition

- Operations
- Information security
- Payment systems
- Outsourcing

4.4 Approach of Croatian National Bank

Since the Riječka bank loss, Croatian state institutions and wide public clearer understood that information system audit must be unavoidable component of each audit. It became obvious that improvement of information technology control and audit is necessary and that information systems audit is multidisciplinary activity, encompassing knowledge about technology, information systems and business conduct.

Unfortunately, it may be said Riječka banka case contributed more to idea of information system audit and control than any other event or initiative in Croatia. Since that time, Croatian National Bank (CNB) pursued very actively idea of information systems audit and control. Already in 2002, a new Banking Law covered some information systems auditing aspects. Also, Specialized On-Site Supervision department was established. That department, among other activities, performed information systems audit and control. Furtherly, in March 2006 CNB announced Guidelines on Information Systems Management in Order to Mitigate Operational Risk and Guidelines for Adequate Management of Outsourcing Risks. In July 2007, decision on adequate information system management was issued. All banks are obliged to act in accordance to these legal documents (law and decision) while guidelines show directions in which CNB will further proceed with legal acts concerning information systems audit and control.

4.4.1 The Banking Law

The Banking Law, which was proposed by CNB, accepted by the Croatian parliament and came into force in July 2002 was the first law in Republic of Croatia which dealt in more details with operational risk and information systems auditing. These subjects were introduced largely as a consequence of events in Riječka banka uncovered a few months earlier.

In article 67, all risks that banks should manage and mitigate are numbered. One of the mentioned risks is “operational risk, including a risk of inadequate management of information technologies and other related technologies”.

Internal audit was named as important factor in information systems auditing. In article 107 it is stated “The internal audit shall conduct ongoing supervision of the entire operations of the bank for the purpose of verifying whether the bank... systematically manages risks arising from business activities of the bank in accordance with the principles of stable operations, including the management of resources of the information technology and other related technologies”.

Furtherly, commercial or “certified” auditors are obliged to perform information systems auditing. In article 114, it is clearly noted that “in the course of conducting an audit certified auditors” should, among other duties, examine and give opinion on “the information system of the bank in accordance with the internationally accepted standards for the audit of information systems”.

The Banking Law also gives guidelines to supervisory audits performed by CNB. In article 115 it is stated that “in discharging its supervisory functions the CNB shall assess the lawfulness and regularity of bank operations, capability of a bank to manage operating risks”. This law also defines on-site supervisory audit function and sets out that banks are obliged to enable the central bank’s auditor to control “of the information technology and other related technologies” (article 119). It also ensures the prerequisites of use of computer assisted auditing tools: “The bank shall also provide the authorized person with the standard interface providing access to the system for database management used by the bank, for the purpose of conducting an examination supported by computer programs” (article 119). That means banks must ensure interface which will enable CNB auditors to apply CAATs on database instances in order to check data and records for omissions, errors and possible frauds. Mentioning of "standard interface providing access to the system for database management used by the bank" and especially important "examination supported by computer programs" is the first appearance of such terms in any legislative act of Republic of Croatia. Since then, CNB auditors regularly use CAATs and corresponding computer assisted auditing methods in their auditing work i.e. analysis of data and records describing business events stored in databases. Computer assisted auditing methods that are used are based on certain CAATs acquired by the CNB. The use of

CAATs and corresponding computer assisted auditing methods by the CNB are the consequence of CNB's assurance that CAATs and underlying methods are extremely effective and that they should be compulsory in any information systems auditing in banks.

Article 122 defines obligation of the banks in the area of "examination of computerized business books and records". Banks must insure that central bank's auditor has at "disposal all that is necessary to gain an insight into:

1. all prescribed activities and procedures of the information system control at the levels of: (a) the bank, (b) management functions, (c) individual business processes and (d) transactions;
2. activities and procedures for the development, acquisition and maintenance of the information system;
3. policies and procedures for the safety of the information system and data protection."

The complex question of change management tracking is touched in article 122: "Any change in program solutions shall be documented in the time sequence of the creation of changes together with the day of the change."

This Banking Law was a solid basis for development of guidelines, decisions and legal documents that were to follow. CNB was aware of operational risks particularly of the risks arising from inadequate development, use and maintenance of banking information systems thus other legal documents covering this subject followed. One of very important issues covered by this law is necessity of ensuring interface to CAATs used by CNB auditors in commercial banks' databases.

Specifically important document that was issued by the CNB in accordance with previously explained Banking Law are Guidelines for Management of Information System in Order to Mitigate Operational Risk. Guidelines covered nine domains of banking information systems and explained what types of activities are indispensable in order to improve information systems management and to mitigate risks. These domains are: organization of information management; risk assessment, mitigation of risks, controls, information classification; internal audit function; security of information system; maintenance of information system; business continuity planning; system development and outsourcing; e-banking systems. Guidelines are the first document produced by any

governmental or public institution which in more details describes how business entities should manage and mitigate risks within their information systems. That document is the consequence of CNB's understanding of information systems importance within any commercial bank and CNB's strong commitment in improvement of those information systems in banking community by means of auditing methods and underlying guidelines and legally binding documents.

4.4.2 Decision on Adequate Information System Management

The Decision was enacted in July 2007 by the Governor of the CNB. It was an effect of Guideline described in chapter 4.4.1, with the important difference that Decision norms are mandatory i.e. they must be fulfilled within certain time limits, while guidelines are advices on certain subject and are not obligatory. Generally speaking, central banks' guidelines always precede legally binding acts and decisions thus giving some time to banks to take steps for alignment with central banks' strategies and norms. The Decision regulates the requirements related to management of information systems of the banking institutions and thus serving as a basis for supervisory audits performed by the CNB audit experts.

Article 2 comprises of comprehensive definitions of terms like software and hardware components, information assets, information technology and system, information system users and risks, properties of information and processes (confidentiality, integrity, availability, authenticity, non-repudiation, verifiability, reliability), controls (administrative, logical, physical), access rights management, audit trails, malicious code, electronic banking, outsourcing, incident, recovery time objective, critical business processes and backup data copies.

Then, set of articles (3 to 11) governing framework for information system management are defined. Bank's management board must nominate one board member responsible for development and supervision of information system management process. It must enact information system strategy which has to be in accordance with business strategy. Internal regulations which govern information system management together with responsibilities for the supervision of their implementation must be adopted. All information system users must be introduced to regulations related to information system according to their delegated needs. Bank must define criteria, methods and procedures for notification of

management and supervisory board about important facts on functionality and security of information system. A role of information system manager must be created by management's board. This role must be independent of the information department manager as well as not under manager's organizational influence. Scope, responsibilities and duties of this role must be established. Management board must appoint information technology steering committee responsible for monitoring and supervising the information system, its operations and compliance with the bank's business goals and business strategy. Furthermore, bank must set up a project management methodology which defines criteria, methods and procedures for managing information system projects.

Information system risk management is covered by articles 12 to 15. Bank must adopt information system risk management process which will include risk assessment, risk mitigation, monitoring and maintaining of the permissible risk levels. The results of information system risk assessment must be documented in the form of a report. Bank must assess and mitigate risks arising from contracts with companies, institutions and individuals who are in some way connected with the bank's information system. Information, data and documents, must be classified and protected accordingly to their sensitivity with respect to integrity, confidentiality and availability.

Internal audit must perform auditing of bank's information system according to defined methodology which will include well established criteria, methods and procedures for information system auditing. In this Decision CNB does not define what methodology must be used, nor gives more details about methodology properties. However, in article 114 of the Banking Law it is stated that information system must be checked and examined "in accordance with the internationally accepted standards for the audit of information systems". That practically means that banks when defining their internal information system audit methodology must follow ISACA, BIS or eventually FED results in this field.

A field of information system security is elaborated in articles 18 to 22. Each bank must adopt its information system security policy which will serve as a framework for information system security management. Responsibilities and roles must be defined for appropriate management of information system security (article 18). Article 19 deals in more details with access control to information system resources: "A bank shall control the access to the information system resources, premises where the information system resources are located and the resources supporting the functioning of the information

system. It shall also apply the appropriate administrative, logical and physical access controls. Special attention should be given to administrative access and remote access to the information system resources." Article 20 furtherly describes the need for system of user access rights management which will include registration, authorisation, identification, authentication and supervision of user access rights. A bank also has to assure the storage of audit trails which will enable auditors of event reconstruction, detection of unauthorised access and bringing conclusions about actions performed on the information system components. Information system components must be protected from malicious code by implementation of suitable logical, physical and administrative controls.

A topic of information system maintenance is dealt with in articles 23 to 26. A bank must set up the process of asset management of information system hardware components during the life cycle of each asset. That process has to include procedures for detection, recording, disposing, monitoring, recovery and discarding the assets (article 23). Change management of business application and system software components is recognized as extremely important. So, banks must establish the procedures for determining the initial versions of software components, monitor all changes in the application software supporting banking services, monitor all changes in the database architecture supporting banking services, monitoring the changes in any other information system component that may affect the functionality or security of the information system. Changes in the monitored software components must be logged in order of their occurrence together with precise time of occurrence. Change management of software components must be supported by testing and approval before their installation on the production platform (article 24). Appropriate procedures for documentation creation, store and maintenance in accordance with the facts must be developed. Bank must ensure that all its employees are adequately and continuously trained for the use of corresponding information system components.

Business continuity management issues are covered in articles 27 to 31. The process of business continuity planning must be established in order to provide availability of critical business processes. Bank must (article 27):

- Create and document a business impact analysis in order to determine the impact on the bank's business of the unavailability of critical business processes and of the information system resources that support those critical processes.

- Establish business continuity plan ensuring the recovery of critical business processes within the maximum allowed time (recovery time objective) and mitigate losses that may arise from interruption of critical business processes.
- Approve disaster recovery plan assuring the recovery and availability of information system components necessary for the carrying out of critical business processes within the recovery time objectives;
- Periodically and after significant changes in the business processes or information system resources, perform the appropriate testing of the business continuity plan and disaster recovery plan. Written reports about testing results must be prepared.

A bank must establish incident management process in order to ensure quick response and recovery in the case of security breaches or discontinuity of information system resources supporting critical business processes. A bank must inform CNB of all major incidents together with its effects and actions taken. Backup storage management process must be defined and approved. It has to include procedures for creating, storing, verifying and restoring backup data copies in order to provide the recovery of critical business processes within recovery time objectives. In accordance with bank's risk assessment, secondary location for backup storage must be set up at a sufficient distance from primary location (article 30). A bank has to prepare and put into work backup (secondary) computer centre with necessary information technology equipment in accordance with business impact analysis and risk assessment. The backup computer centre must be located at sufficient distance from primary computer centre, in the alignment with risk assessment (article 31).

Information system development and outsourcing topics are covered in more details in heading IX. A bank has to define methodology for information system development while stressing the importance of functional and security aspects. Information system methodology must be coordinated with approved project management methodology. Information system development methodology must consist of procedures for analysis and design, programming, testing and releasing into production environment. All system software, application modules and IT hardware components must be appropriately tested and formally accepted before production release. For those reasons bank must set up separate development, testing and production environments. A bank has to check if legislation of the country in which service provider operates allows the CNB to perform its supervisory duties without any restrictions, before any decision about outsourcing of

information system component is made. Before decision about outsourcing, bank has to assess the risks related to outsourcing arrangement. A bank must monitor the way and quality of providing outsourced services.

Concerning the electronic banking (heading X.), a bank must implement secure authentication methods in order to authenticate the identities of individuals, processes and systems. Whenever it is applicable, authentication procedure must include a combination of at least two factors of user identification. A bank must assure their clients of its identity in the electronic banking applications so that users can verify the bank remotely. Adequate audit trails must be stored in order to ensure the non-repudiation of client's and bank's activities.

Although the Decision was enacted by Governor in 2007, majority of articles entered into force on 1st of January 2008. Entering into force of articles that require more preparation, financial and organizational activities was postponed to 1st of July 2008, 1st of January 2009, 1st of July 2009, 1st of January 2010 and 1st of July 2010. It is important to stress that although Decision deals with definition of obligatory tasks for adequate information system management within banking industry, it serves as a basis for information system audits performed by the CNB.

4.5 Conclusion on Existing Frameworks and Approaches

In contemporary business environments, information systems auditors are requested to add extra value to auditing activity and business entity being audited. It is usually demanded by auditee itself, but also by legislative authorities i.e. laws and acts. These demands are especially enforced after enormous losses and a number of bankruptcies. Auditors are compelled to examine not only general information systems controls in order to confirm if information system is in general terms adequate and that certain activities have been undertaken that decisions can be based on data and reports from information system. They are forced to examine data and processes in details in order to prove that information system is reasonably resistant to fraudulent activities, omissions and errors.

That means that auditors must clearly understand business and information systems processes, weaknesses in specific control mechanisms, fraud, omission and error

indicators, necessity for monitoring these indicators and be ready and willing to perform additional auditing and investigation when certain indicators are recovered.

Auditors also have constantly increasing responsibility to appropriately document and store their findings and to be prepared to go to court in order to help eventual prosecutions.

Modern information systems are complex and usually have many software, hardware and organizational components that should fit together to produce appropriate business solution. Assurance that information system is without weaknesses can be accomplished only if all its components are appropriately audited. It is of a major importance that information systems auditing encompasses [23]:

1. Physical and environmental review - Physical security, power supply, air conditioning, humidity control and other environmental factors.

2. System administration review - Security review of the operating systems, database management systems, all system administration procedures and compliance.

3. Application software review - access control and authorizations, validations, error and exception handling, business process flows within the application software and complementary manual controls and procedures. A review of the application development lifecycle must be completed.

4. Network security review - internal and external connections to the system, perimeter security, firewall review, router access control lists, port scanning and intrusion detection.

5. Business continuity review - existence and maintenance of fault tolerant and redundant hardware, backup procedures and storage, and documented and tested disaster recovery/business continuity plan.

6. Data review – checking of validity, completeness and integrity of business data in order to verify adequacy of controls and impact of weaknesses, as noticed from any of the above reviews. Such substantive testing should be done using computer assisted audit techniques.

All abovementioned auditing areas must be thoroughly audited in order to present to management a clear assessment of the system. It is possible to have first five components almost perfect, that business application solution is developed according to user

(functional) specification but at the same time data entry controls are not appropriate. In that case, information system is designed as it is defined by business function which means it is aligned with business. However, such information system can lead to high number of omissions, errors and even frauds or losses.

Moreover, for example network security towards public networks may have been implemented sufficiently well, but the access privileges to operating system supporting internal business applications may have been adversely implemented. If access privileges enable unauthorized employees with access to execute or even change certain application components, then risks of inappropriate use of applications grow enormously. Some examples of notorious frauds are explained in chapter 2.

It is important to emphasize that audit process can be consisted of these components in different intensity. In the practice, certain audit proceeding is often focused only on one of above numbered components i. e. some of them are usually omitted. However, it is obligatory to execute all components, but it is not always feasible to perform all of them at once in one audit assignment. It is necessary that auditor and management judge the results of each audit assignment in mutual relationship, as one complete audit proceeding. Only then it is possible to adequately asses if information systems component of operational risk is appropriately mitigated.

Data, usually stored in databases and managed by database management systems, is of a major importance for any business organization. Business decision making is strongly based on data produced within or outside organization. If data on which business decision-making process relies upon are erroneous or incorrect, than decisions are obviously not made on appropriate basis. This may lead to huge financial losses, bankruptcies of businesses and even systemic disorders in state, regional or even global economies. Some of such notorious cases are described in chapter 2.

Furthermore, number of transactions and data stored in databases is constantly and quickly increasing. Also, the way businesses are conducted i.e. business processes is getting more and more complicated. For example, number and complexity of financial instruments (bonds, loans, bills etc.) in financial industry is significantly increased in last years. This means that business processes that should be managed are considerably more complicated. As business processes are producing more and more data with increased complexity it is

obvious that it is not possible to perform the data audit without computer technology based tools. Also, accordingly to importance of data in management of any business organization, it is necessary to give special attention to data checks and analysis i.e. to control and auditing of business data. So, more advanced approaches which will not be exclusively based on manual controls and analysis of certain data samples must be implemented throughout auditing process. Practically, such large data sets that became regular in today's business environments must be analyzed and checked with specialized computer (software) tools. Such specialized computer based tools that assist in data audits already exist on the market under the name of CAAT (computer assisted auditing tools). As a minimum, CAAT must have specific built in functions for data audit like selection, extraction, join, summarization, stratification, calculated columns, duplication detection, rounded values, gaps, Benford's Law etc.

As it is briefly noted in chapter 4.1.1, ISACA issued guideline "G3 Use of Computer Assisted Audit Techniques (CAATs)" in order to set direction in which computer assisted auditing should be developed. Guideline emphasised that the use of CAATs should be controlled by the auditor to provide reasonable assurance that the audit objectives and the detailed specifications of the CAATs have been met. The auditor should:

- Perform a reconciliation of control totals from different data sources if appropriate
- Review output for reasonableness
- Perform a review of the logic, parameters or other characteristics of the CAATs
- Review the organisation's general information system controls, which may contribute to the integrity of the CAATs (e.g., program change controls and access to system, program, and/or data files)

When using test data, the auditor must be aware that test data only point out the potential for erroneous processing since this technique does not evaluate actual production data. The auditor should also be aware that test data analysis can be extremely complex and time consuming, depending on the number of transactions processed, the number of programs tested and the complexity of the programs/systems. Before using test data the auditor should verify that the test data will not permanently affect the live system.

When using generalised audit software to access the production data, the auditor should take appropriate steps to protect the integrity of the organisation's data. With embedded audit software, the auditor should be involved in system design and techniques should be developed and maintained within the organisation's application programs/systems.

When using utility software, the auditor should confirm that no unplanned interventions have taken place during processing and that the utility software has been obtained from the appropriate system library. The auditor should also take appropriate steps to protect the integrity of the organisation's system and files since these utilities can easily damage the system and its files.

Customised queries or scripts allow the auditor to specifically target desired information for analysis. Customised scripts are highly useful for environments where other CAATs are not available but usually require specific technical skill sets to create them. Therefore, the auditor should obtain assurance of their integrity, reliability, usefulness and security through appropriate planning, design and testing before reliance is placed on CAATs, and ensure that proper source data are used and that output from scripts and queries are in the proper format. Customised query and script code should be maintained in a secure location to prevent unauthorised changes from occurring.

When using application software tracing and mapping, the auditor should confirm that the source code being evaluated has generated the object program currently being used in production. The auditor should be aware that application software tracing and mapping only points out the potential for erroneous processing; it does not evaluate actual production data.

The auditor must use and document the results of appropriate procedures to provide for the ongoing integrity, reliability, usefulness and security of the CAATs. For example, this should include a review of program maintenance and program change controls over embedded audit software to determine that only authorised changes have been made to the CAATs. When CAATs reside in an environment not under the control of the auditor, an appropriate level of control should be in effect to identify changes to the CAATs. When CAATs are changed, the auditor should obtain assurance of their integrity, reliability, usefulness and security through appropriate planning, design, testing, processing and review of documentation before reliance is placed on the CAATs [45].

Although ISACA, as a leader in field of information systems auditing, promotes CAATs and issued before mentioned guideline G3, appropriate strict and detailed methodology for computer assisted auditing is still not established. As a consequence, auditors implement CAATs according to guidelines, approaches or directions defined by their local legal authorities. Although these documents give certain overview and highlights how CAAT should be used at the same time they lack necessary depth and details. Simply, there is no methodology containing the definition of methods, their way of use and mutual relationships.

So, such methodology should consists of appropriate and effective methods for data audit and model containing steps of methods usage, their relationships, inputs, outputs and possible conclusion-making process. One of key steps in process of methodology development is choosing adequate methods. Lately, Benford's Law earned attention and focus of some auditors and academy researchers. As it is already stated in [10], [17] and some other works, Benford's Law may be very useful in auditing of information systems so it is chosen as a principal method of methodology being developed in chapter 7. In chapters 5 and 6 extensive explanation of Benford's Law properties, various tests and conformance criteria are given.

Apart from Benford's Law, adequate methodology for computer assisted information systems auditing should consist of some other methods enabling efficient execution of audit process. Specific methods that proved efficient in practice of data extraction and analysis can also be very useful in audit process based on data audit. These methods that are candidates for use in specific computer assisted information systems auditing methodology are explained in the following chapter.

5. Analysis of Particular Methods for Computer Assisted Information Systems Auditing

There are number of methods used in process of computer assisted auditing. Some of these methods are even supported within computer assisted auditing tools which improves their strengths and capabilities. Methods are outcome of frameworks and approaches described in chapter 4 and are regularly used in computer assisted auditing activities. The list of methods that follow is certainly not final and often combinations of methods are used:

- Append - It merges two data tables with identical columns into a single data table. An example would be to append two sets of rows from different periods stored in two data tables into one data table. Append is similar to union relational operator with a difference that append operation does not exclude duplicated records from newly formed data table.

- Index/sort - A content of a data table is sorted in ascending or descending order on certain columns. If more than one column is chosen for a sort, it will be performed in the order of choice. Ascending and descending sorts may be combined.
- Summarize - This method totals numeric columns based on a specified key column. One example is totalling invoice amounts (summarization column) by supplier number. This method is explained in more details in chapter 5.4.
- Calculated column or field – A variety of spreadsheet like statistical or mathematical functions are necessary property of CAATs. Examples of these functions are standard arithmetical operations (addition, subtraction, multiplication, division, exponential calculation, roots), calculation of absolute values, counting of values, average etc. A calculated column or field is based on the data within table.
- Duplication detection - Duplicate values are extracted within a specified data columns. For example, this method can be used to find eventual duplicate invoices paid within the purchase data table. More on duplication detection method can be found in chapter 5.6.
- Selection (extraction) - Specified records are extracted from data table in order to ease the search. Selection is carried out using so called “where” clause which

contains condition. Within CAAT, selected data are usually copied to another data table. Further explanation of this method can be found in chapter 5.2.

- Gaps – Method is used for identification of cuts in a specified column in data table. Using this method, auditor may easily search for gaps in column which values, when sorted, should form sequential array without any break. For example, method can find missing customers from within account receivables in certain period of time.
- Join - Specified columns from two data tables are combined into a single table using values in key columns used for comparison. For example, table with all master data on banks could be related to the payment transactions table using equality expression between bank code columns in both tables. This method is explained in more details in chapter 5.3 and used in methodology developed in chapter 7.2.
- Stratification – This method counts the number and value of table records falling within intervals predefined by auditor. Stratification method provides very useful view into the data, providing help for data and business conduct understanding. A method is explained in more details in chapter 5.5 and used in methodology explained in chapter 7.2.
- Benford's Law – It is designed to find abnormal deviations of specific digits in values, as well as deviations in digit combinations in certain number sets. It is furtherly used to find abnormal duplication of values or clustering around specific limits. Benford's Law defines the expected frequencies of the digits in value data sets if data are authentic and non-manipulated. Benford's Law is explained extensively in chapters 6 and 5.1 and represents the basis of the computer assisted information systems auditing methodology designed and verified in chapter 7.
- Rounded values - this method produces sorted list of number values rounded to multiplies of 5 or 10. Rounded values are sorted descending according to frequency and rounded value itself in descending order. More detailed explanation is presented in chapter 5.7.
- Horizontal analysis - This method analyzes the increases and decreases in balances, normally financial statement, over two or more periods. Examples are calculations for balance sheet, income statement and/or budget-to-actual analysis data.

- Vertical analysis – It examines balances, normally in financial statements, in a single period where each balance asset value is shown as a percentage of the total assets and every income value is shown as a percentage of the total sales.
- Trend analysis - This method includes comparing any of the analytical tests over two or more periods. It is used to measure whether the data in a selected numeric data table column shows upward or downward trend in time and then to define the best fitting straight line. Trend is also used to forecast values on the assumption that the trend pattern i.e. straight line will continue in the future. The use of trend analysis is very important in any fraud detection because fraudulent transactions often create deviations in time that could go undetected if only the single year were being analyzed and if no trend straight line would be defined.
- Correlation – This method, also called correlation coefficient, is a measure of the strength and direction of a relationship between the values in two numeric table columns. In other words, correlation method is utilized for determination how closely the values in two numeric table columns are related.
- Regression – Calculates a dependent column value (e.g. payment amount) based on number of independent column values (e.g. bank code, type of transaction, country of payment etc.). Regression also ensures specific precision percentage for each test so that the auditor can assess the reliability of the test.
- Pivoting – Pivoting method is an interface to data tables in which auditor may define how data is displayed and organized. Auditor defines rows and columns which should be displayed, together with aggregation totals according to specific conditions.
- Sampling – CAAT should include a few methods of sampling (e.g. systematic or interval, random, stratified random sampling). Sampling can be used if number of records being audited becomes too large for a computer power auditor has in possession.

According to previous research, status of auditing approaches, frameworks and experience, conclusions about specifically adequate computer assisted auditing methods can be made. Specifically useful auditing method which is used in auditing processes only lately and still quite scarcely is Benford's Law.

Benford's Law, as it is explained in more details in [6], [8], [10], [11], [17] and [19], includes a number of tests. Especially valuable are first digit test, second digit test, first two digits test and first three digits test. These tests proved to be extremely efficient in practical auditing process. They can improve investigations on data in a sense that auditor does not have to initially define what type of fraud, omission or error is being investigated. After Benford's Law tests are applied on data, auditor can reasonably easy notice deviations which afterwards have to be compared to business rules and further explained. Various Benford's Law tests enable different focuses on audit data as well as efficient check of complete data set being audited. For these reasons, Benford's Law is the central method in model of methodology designed in this paper.

Selection method is irreplaceable when speaking of methods for analysis, filtering and extraction of data. It is a basic operation of relational algebra used for focusing on certain attributes (data columns) and rows (records, tuples). Join method is also one of basic and indispensable operations of relational algebra. It enables relating ("connecting") different tables with common attribute(s). Summarization ensures grouping of data according to unique values in selected attributes and performs chosen mathematical functions on some other attributes. Stratification method produces counts, percentages and other mathematical functions based on pre-defined data layers. The objective of duplication method is to find duplicated values in certain attribute(s) thus identifying value (usually number) invention. Rounded values method produces descending ordered list of numbers rounded to multiplications of 5 or 10, which can be very useful in identification of estimation.

According to experience and assessed usefulness of methods, previously numbered methods are used within created methodology. So, methods that constitute computer assisted information systems auditing methodology developed in this paper are:

1. Benford’s Law
2. Selection
3. Join
4. Summarization
5. Stratification
6. Duplication
7. Rounded values

5.1 Benford's Law

As it is described in more details in chapter 6, Benford's Law defines expected digit frequencies in certain number sets. It is noticeable that in sets of numbers from many data sources, certain digits are distributed in a particular way. According to the first digit Benford's Law, digit "1" appears as the first digit in number for almost one third of the time, and larger digits appear on the leading number position with lower and lower frequencies. E.g. digit 9 appears as a first digit in slightly more than 4,5% numbers. The basis for Benford's Law lies in the fact that values of real world data sources are often distributed logarithmically, thus the logarithm of this real world data sources is distributed uniformly. Benford's Law may be applied to the first, second, first two and first three digits in numbers. That is why there are in fact four methods based on this law: the first digit test, the second digit test, the first two digits test and the first three digits test.

Benford's Law of the first digit i.e. probability P of appearance of digit z_1 in number system with base 10 on leftmost position in number can be expressed by the following formula:

$$P(z_1)=\log_{10}(1+1/z_1),\ z_1 \in [1..9] \qquad (1)$$

Formulas for probabilities of appearance of the second, first two and first three digits in number system with base 10 are:

$$P(z_2)=\sum_{z1=1}^{9} \log_{10}(1+1/z_1 z_2),\ z_2 \in [0..9] \qquad (2)$$

$$P(z_1 z_2)=\log_{10}(1+1/z_1 z_2),\ z_1 z_2 \in [10..99] \qquad (3)$$

$$P(z_1 z_2 z_3)=\log_{10}(1+1/z_1 z_2 z_3),\ z_1 z_2 z_3 \in [100..999] \qquad (4)$$

Each of these methods uses certain numeric attribute as input and counts frequencies certain combination of digits, depending on specific method. Output is list of all digits combinations and their respective frequency.

5.2 Selection

Selection is one of operations of relational algebra which is used for extractions (or selections) of data that holds for defined condition. Selection is very powerful operation which is most commonly used query-based operation in business application software.

In relational algebra, selection (sometimes called restriction or exclusion) is a unary operation written as $\sigma_{xOy}(r)$ or $\sigma_{xOc}(r)$ where:

- x and y are relation's attribute names
- O is a binary operation in the set (greater than, greater or equal than, equal, not equal, lesser than, lesser or equal than). It may also consist of logical Boolean operators (AND, OR, NOT).
- c is a constant
- r is a relation

The selection $\sigma_{xOy}(r)$ selects all rows in r for which O holds between the x and the y attribute.

The selection $\sigma_{xOc}(r)$ picks only rows in r for which O holds between the x attribute and the constant value c.

In database management systems, selection relational algebra operation is designated by SELECT SQL statement. That statement extracts all rows (records, tuples) from a table (term “table” in database management system terminology corresponds to term “relation” in relational algebra) whose attributes hold against selection criteria:

t2 = select(t1,P)

Table t2 is created out of table t1, and it contains only rows from table t1 which satisfy (or hold against) the predicate P.

A predicate is simply an expression made out of Boolean algebra whose operators are the logical Boolean expressions (and, or, not) and arithmetic expressions (<, <=, >, >=, =, <>), and whose operands are either attribute names or attribute domain constants. A predicate may also represent another select statement thereby producing relation nesting. In practice, selection is usually used together with projection operation. Projection operation includes only chosen attributes out of table (relation) and may include mathematical functions over included attributes (e.g. maximum, minimum, average).

Input data for selection method is table (or relation in relational algebra terminology). Selection’s predicate in fact represents method’s algorithm. Output of selection is again table, restricted on only those rows which satisfy predicate.

Selection method is very powerful and it is mandatory in computer assisted auditing. Without this method, it is not possible to effectively audit business activities. This is true even if audits are performed without computer assisted auditing tools.

5.3 Join

Join is operation of relational algebra which is fundamental to the model. It would not be possible to decompose data structure into number of relations if there would not be a method for their composition when necessary. This is precisely what a join operator performs. It combines rows based on the comparison of one or more common attributes in both relations in join. It is written as

$r \underset{x\theta y}{\bowtie} s$ or $r \underset{x\theta c}{\bowtie} s$

where r and s are relations, x and y are attribute names of relation. Also, instead of y, constant c may be used.

Join operations can be classified as theta, equi-join, natural and outer (or external) join.

Theta (θ) join means that its result follows the general definition of the join operation. Theta is a predicate which consists of one of the binary operators in the set (greater than, greater or equal than, equal, not equal, lesser than, lesser or equal than) and specifies the join condition. If join condition θ equals "=", the operation is called an equi-join. Natural join is in fact equi-join from which duplicate attributes used for join are excluded. The resulting joined relation contains only one attribute for each pair of attributes holding same data.

Outer join does not require each data row in two joined relations to have a matching record. Resulting joined relation holds each row from at least one of relations even if no corresponding matched row exists, depending on outer join type. There are three types of outer joins: left outer joins, right outer joins, and full outer joins. The resulting relation of a left outer join (or shorter "left join") always contains all rows of the left relation (r), even if the join condition does not find any relating row in the right relation (s). So, left outer join always returns all rows from the left relation (r) together with rows from right relation (s) matching according to θ condition. If there are no matching rows in right relation (s), attributes of right relation (s) will contain only NULL values. If the right relation (s)

returns more than one matching row for certain row in the left relation (r), the rows in the left relation will be repeated for each distinct row on the right relation (s).

The opposite case holds for right outer join (shorter "right join"). In case of full outer join, result is union of theta join, left and right joins. One should bear in mind union is a set operator, so all rows that are eventually identical in separate relations which are members in union (theta, left and right) will remain only in one instance in resulting relation.
There is no explicit notation for outer join operations in standard SQL. However, it is easily implemented in all modern databases by combination of expressions based on Boolean operators.

5.4 Summarization

Summarization method aggregates amounts of interest according to specific attributes (or columns in SQL notation). Summarization extracts and group all different attribute values chosen by auditor and aggregate according to defined attributes. Auditor must define which attributes have to form unique combination of values (aggregation base attributes), which attributes have to be aggregated on (aggregation value attributes) and what summarization function has to be performed (aggregation function). For each unique extracted row value of aggregation base, summarization is executed for aggregation value attributes according to aggregation function. Notation is as following:

$$S_{AB,AV,f}(r)$$

S stands for summarization method, AB stands for aggregation base attributes, AV denotes aggregation value attributes, f is aggregation function, while r is relation. There are number of aggregation functions that can be applied: average value, sum of amounts, count of rows, minimum value, maximum value etc. Auditor has to remember that each combination of aggregation base attributes shows up in resulting relation only once, and attributes representing aggregation value hold result of aggregation function for all rows with same aggregation base attributes value.

Selection and join methods may be used in order to prepare data i.e. to extract and add additional attributes to final relation ready for summarization.

In SQL, summarization method may be represented with GROUP BY statement. The GROUP BY statement is used in conjunction with the aggregate functions to group the result-set by one or more columns.

5.5 Stratification

Stratification method includes creation of specific data strata (data layers) in accordance with defined value-based categories. As input parameters, method uses relation, attribute and strata limits. So, auditor has to choose which column is of special interest (usually number or date data type), define number of strata and their limits (upper and lower values).

It is not required that auditor should include all values of certain relation's attribute (table column) when applying stratification method (from minimum to maximum value). All rows are included in respective data strata, depending on values and strata limits. After stratification method is performed, auditor may investigate each stratum and make conclusions on data characteristics. This method is especially useful if combined with exception analysis. Auditor may learn about limit values for certain table columns and then additionally analyze column values and rows out of limiting bounds. Notation of stratification method (ς) is:

$$\varsigma_{x,l}(r)$$

where x stands for attribute for which strata should be created while l denotes set of boundaries (lower and upper bound) for each strata.

Method processes each table row and classifies it into corresponding strata, depending on attribute value x. Both totalling and counting functions may be applied on attribute x, and assigned to certain strata which results from pre-defined limit values. Method results in:

- count of rows and totalling of attribute values belonging to each strata
- calculation of percentage of rows in each strata in relation to total number of rows
- counting of all rows with attribute x value lesser than the lowest strata boundary (lowest limit exceptions) and greater than the greatest strata boundary (greatest limit exceptions); percentage of both values in relation to total number of rows; totalling values of attribute x below and above lowest and greatest limit exceptions
- percentage of totalled value for each strata in relation to grand total for all rows

After performing calculations on rows and values of each stratum, auditor may be introduced to a profile of the data in the database. Then, auditor may easier analyze any discrepancies from expected trends.

5.6 Duplication

Duplication method checks for numeric values (amounts) which appear more than once in attribute of interest of certain relation. As input parameters, method uses relation (r) and attributes (x) of interest, and its notation is:

$$D_x(r)$$

Usually, only one attribute for duplication values check is chosen. This method finds all values in chosen attribute that have multiple appearances in relation. Output of these values is sorted according to number of appearances in descending order and value in descending order. The objective of this test from auditing perspective is to find relatively small groups of recurring numbers. As it is shown in [17], when people invent numbers, they often tend to repeat values. This may be of major significance to auditing process. This test is usually performed only on value subsets which have excessive positive deviations in first two and first three Benford's Law tests.

5.7 Rounded values

Rounded values method finds numeric values (amounts) which are rounded to multiples of 5 or 10. Of course, method may be extended to multiples of 100, 1000 etc. which are all multiplies of 10, or to 25, 75 etc. which are all multiplies of 5. Notation is:

$$R_{x,m}(r)$$

where x is numeric attribute, m is multiplication value and r is relation. Method checks values of attribute x for all rows in relation and checks if value is multiplication of m. In fact, method searches for values in x that are divisible by m without remainder. Method also counts recurrences of all rounded values. Method's output is sorted by frequency of rounded values in descending order and rounded value itself in descending order.

This method looks for abnormal repetition of rounded values because such findings may be proof of estimation. Estimation is usually strongly related to omissions, errors and even fraud.

5.8 Conclusion on Methods for Computer Assisted Auditing of Information Systems

Methods explained in chapters 5.1 through 5.7 are proved to be very efficient in audit processes. They form significantly broad scope for efficient data analysis which can be used for fraud, error and omission detection. In Table 1, overview of methods is presented by description of their objectives, inputs and outputs.

Method	Objective	Inputs (I) and Outputs (O)
Benford's Law First Digit Test (BL FTD)	Finding actual frequencies and deviations from BL FDT frequencies	Attribute of relational table containing number values (I) 9 subsets for digits 1-9 with actual frequencies and corresponding deviations (O)
Benford's Law First Two Digits Test (BL FTDT)	Finding actual frequencies and deviations from BL FTDT	Attribute of relational table containing number values (I) 90 subsets for digits 10-99 with actual frequencies and corresponding deviations (O)
Benford's Law First Three Digits Test (BL FThreeDT)	Finding actual frequencies and deviations from BL FThreeDT	Attribute of relational table containing number values (I) 900 subsets for digits 100-999 with actual frequencies and corresponding deviations (O)
Benford's Law Second Digit Test (BL SDT)	Finding actual frequencies and deviations from BL SDT	Attribute of relational table containing number values (I) 10 subsets for digits 0-9 with actual frequencies

		and corresponding deviations (O)
Selection	Selecting rows satisfying WHERE criteria	Rows of relational table (I) Rows of relational table satisfying WHERE clause criteria (O)
Join	Combining rows from two relational tables according to join type	Rows of two relational tables usually with at least one common attribute (I) Rows of newly formed temporary relational table satisfying join type and criteria (O)
Summarization	Grouping and aggregation of rows	Rows and attributes of relational table, aggregation functions (I) Rows grouped on unique attribute values, aggregated on selected attributes with certain aggregation function (O)
Stratification	Creation of data layers according to pre-defined limits	Rows and attribute of relational table, strata limits, mathematical functions (I) Data layers with counted and summarized rows together with calculated percentages for chosen attribute (O)
Duplication	Finding numeric values which appear more than once in attribute of interest	Rows and attribute of relational table (I) Rows grouped and sorted descending by frequency and descending by numeric value of chosen attribute (O)
Rounded Values	Finding rounded numeric values in attribute of interest	Rows and attribute of relational table (I) Rows grouped and sorted descending by frequency and descending by numeric value of chosen attribute (O)

Table 1. Methods and corresponding objectives, inputs and outputs

Although the efficiency of individual methods listed in Table 1 in practice proved to be out of question, they are used individually in accordance with abilities and judgement of auditors. There is no strict sequence of their usage, no steps and mutual relationships are defined. Since no methodology is defined that will relate and order described methods when performing audit process, each auditor uses them in different setting. The consequence is that auditors use different methods in various sequences with possibly inconsistent input data and results. This is a fact even if the same computer assisted auditing tool is used in two different audits, and even if the same business process and data are being audited. Also, the same auditor using the same computer assisted auditing tool processing the same business process and corresponding data but in two different actual audits can produce completely different results which can lead to very different conclusions. Without adequate methodology, auditing processes are hardly comparable and comparability of audits is of a major importance. Additionally, inappropriately applied methods, their mutual relationships and possibly wrong conclusions made by auditors result in inadequate audits.

In order to improve audit process, adequate computer assisted information systems auditing methodology should be developed on the basis of abovementioned methods. Since Benford's Law will represent a basis of this methodology, its usage will be investigated and described in details. The advanced capabilities of different Benford's Law tests (the first digit, the first two digits, the first three digits and the second digit) will be presented in the following chapter. Methodology for computer assisted information systems auditing, consisting of methods described in chapter 5, will be designed and verified in chapter 7.

6. The Role of Benford's Law in Information Systems Auditing

6.1 Definition and Description

Benford's Law defines expected digit frequencies in certain number sets. The most often works in literature focus on Benford's Law for first digit. That is probably why it is often called „First Digit Law", „First Digit Phenomenon" and „Leading Digit Phenomenon". However, digits on any position in a number sets will follow certain probability of appearance.

The first or leading digit in a number is leftmost positioned digit, i.e. digit with the most value. For example, in number 205, digit "2" is the first digit. It is clear that digit "0" is not possible as a first digit but can appear on second and consecutive positions.

It is noticeable that in sets of numbers from many data sources, leading digit is distributed in a particular way. According to Benford's Law, digit "1" appears as the first digit in number for almost one third of the time, and larger digits appear on the leading number position with lower and lower frequencies. E.g. digit 9 appears as a first digit in slightly more than 4,5% numbers. The basis for Benford's Law lies in the fact that values of real world data sources are often distributed logarithmically, thus the logarithm of this real world data sources is distributed uniformly.

So, Benford's Law opposes uniform distribution since it states that in certain number sets, for example digit "1" will occur on leftmost position with probability of around 30,1% which is much greater than the expected 11.1% (i.e., one digit out of 9) according to uniform distribution. It is confirmed that this counter intuitive result can be applied to a wide variety of data sets and that it even holds to any base of numeric system. Of course, when changing number bases, actual digit distributions will change. Benford's law states that the leading digit z ($z \in [1..b-1]$) in base b ($b \geq 2$) occurs with probability $P(z)=\log_b(z+1) - \log_b z = \log_b((z+1)/z)$.

Benford's Law of first digit i.e. probability P of appearance of digit z_1 in number system with base b = 10 on leftmost position in number can be expressed by the following formula:

$$P(z_1)=\log_{10}(1+1/z_1),\ z_1 \in [1..9] \quad (1)$$

Probabilities of each digit on the most significant position in number are shown in Table 2.

digit (z_1)	probability $P(z_1)$
1	0,30103
2	0,17609
3	0,12494
4	0,09691
5	0,07918
6	0,06695
7	0,05799
8	0,05115
9	0,04576

Table 2. Probabilities of each digit on the first position in number according to Benford's Law (base b=10)

It was explained that Benford's Law also applies to other significant digits in numbers. Furthermore, if second digit is observed, probability P of appearance of digit z on 2nd position in number is:

$$P(z_2)=\sum_{z1=1}^{9}\log_{10}(1+1/z_1z_2),\ z_2 \in [0..9] \quad (2)$$

Probabilities of each digit on the second most significant position in number are shown in Table 3.

digit (z_2)	probability $P(z_2)$
0	0,11968
1	0,11389
2	0,10882
3	0,10433
4	0,10031

5	0,09668
6	0,09337
7	0,09035
8	0,08757
9	0,08500

Table 3. Probabilities of each digit on the second position in number according to Benford's Law

Also, Benford's Law defines following rules of appearance of first two (3) and first three (4) digits in number:

$$P(z_1z_2)=\log_{10}(1+1/z_1z_2),\ z_1z_2 \in [10..99] \qquad (3)$$

$$P(z_1z_2z_3)=\log_{10}(1+1/z_1z_2z_3),\ z_1z_2z_3 \in [100..999] \qquad (4)$$

Very interesting examples of Benford's law compliance are shown in [http://mathworld.wolfram.com/BenfordsLaw.html]. Taking data from several disparate sources, the table below shows the distribution of first digits as compiled by Benford (1938) in his original paper.

col.	Title	1	2	3	4	5	6	7	8	9	samples
A	Rivers, Area	31.0	16.4	10.7	11.3	7.2	8.6	5.5	4.2	5.1	335
B	Population	33.9	20.4	14.2	8.1	7.2	6.2	4.1	3.7	2.2	3259
C	Constants	41.3	14.4	4.8	8.6	10.6	5.8	1.0	2.9	10.6	104
D	Newspapers	30.0	18.0	12.0	10.0	8.0	6.0	6.0	5.0	5.0	100
E	Specific Heat	24.0	18.4	16.2	14.6	10.6	4.1	3.2	4.8	4.1	1389
F	Pressure	29.6	18.3	12.8	9.8	8.3	6.4	5.7	4.4	4.7	703
G	H.P. Lost	30.0	18.4	11.9	10.8	8.1	7.0	5.1	5.1	3.6	690
H	Mol. Wgt.	26.7	25.2	15.4	10.8	6.7	5.1	4.1	2.8	3.2	1800
I	Drainage	27.1	23.9	13.8	12.6	8.2	5.0	5.0	2.5	1.9	159

J	Atomic Wgt.	47.2	18.7	5.5	4.4	6.6	4.4	3.3	4.4	5.5	91
K	$n^{-1}, \sqrt{n}$	25.7	20.3	9.7	6.8	6.6	6.8	7.2	8.0	8.9	5000
L	Design	26.8	14.8	14.3	7.5	8.3	8.4	7.0	7.3	5.6	560
M	Reader's Digest	33.4	18.5	12.4	7.5	7.1	6.5	5.5	4.9	4.2	308
N	Cost Data	32.4	18.8	10.1	10.1	9.8	5.5	4.7	5.5	3.1	741
O	X-Ray Volts	27.9	17.5	14.4	9.0	8.1	7.4	5.1	5.8	4.8	707
P	Am. League	32.7	17.6	12.6	9.8	7.4	6.4	4.9	5.6	3.0	1458
Q	Blackbody	31.0	17.3	14.1	8.7	6.6	7.0	5.2	4.7	5.4	1165
R	Addresses	28.9	19.2	12.6	8.8	8.5	6.4	5.6	5.0	5.0	342
S	$n^1, n^2 \cdots n!$	25.3	16.0	12.0	10.0	8.5	8.8	6.8	7.1	5.5	900
T	Death Rate	27.0	18.6	15.7	9.4	6.7	6.5	7.2	4.8	4.1	418
	Average	30.6	18.5	12.4	9.4	8.0	6.4	5.1	4.9	4.7	1011

Table 4. Distribution of first digit – compiled by Frank Benford

American astronomer Simon Newcomb was first who found out that numbers more frequently begin with smaller digits than with greater digits. Newcomb noticed that pages in logarithm tables were dirtier at the start, i. e. more used, and progressively cleaner as approaching to the end. He concluded that numbers more often begin with digit 1 than with any other digit, and in addition, that probability of each following digit (up to 9) at the most significant position in number progressively decreases.

Frank Benford gathered more than 20.000 observations from different sources (geographical area, population, river areas, physical constants etc.). He analysed frequencies of first digits for each number set. After he summarized all individual analyses he concluded that probability of first digit being 1 is 0,30103 which equals $\log_{10}2$, probability of first digit being 2 is 0,17609 which equals $\log_{10}3/2$ etc.

There is rather extensive literature on various fields of usage of Benford's Law. Also, there are numerous works carried out on application of Benford’s Law in information systems auditing.

In [19] it was shown in details how data auditing based on Benford's Law was executed in accounting department. Audit observed 28.736 invoices authorized for payment by the accounts payable system of a business segment. After performing the first digit test it was noted that the largest deviation is for the first digit 1, where the actual proportion exceeds expected proportion by 1,3 percent. However, with the results of Z-statistics it was concluded that the first digit test conformed to properties of Benford's Law. The second digit test shown that digit 0 and digit 5 on the second position in number exceeded those of Benford's Law. It was concluded, since invoices are the selling prices of goods and services, it is not surprising there are excess second digit 0 and 5. It was mentioned that separate digital analysis tests were performed on 1,6 million invoices of US Industrial conglomerate. Performed test shown nearly identical deviations so auditors can expect the same biases when analyzing invoices. The first two digits test (FTD) showed significant excess of 5 two digits combinations which could be result of fraud, errors or processing inefficiencies. As an extension, number duplication test was performed. Authors were focused on 50 most frequent dollar values and additionally observed values that had excess in FTD test. Among other conclusions it was proved that some duplication of values resulted in inefficient way of invoice processing.

In [4] it was explained that FTD test may be used in contract audit. A comparison of the actual contract amounts to expected FTD frequencies according to Benford's Law may highlight a higher than expected occurrence of contracts with amounts starting just bellow sole sourcing limit. Further investigation of these contracts may identify that individuals deciding on sole source contracting is directing them to friends or relatives.

In [20] it is described how Benford's Law principles were used in accounts payable disbursements audit in one federal agency. The first digit test shows that leading digit 1 occurs with a substantially higher frequency than its predicted recurrence under Benford's law. Second step that was conducted was number duplication test for all values with digit 1 at leftmost position. It shown excess of one single value when compared to Benford's Law frequencies.

6.2 Intuitive Explanation

This law is based on assumption that number set sorted ascending forms geometric series.

Furtherly, Benford's law can be clarified under assumption that logarithms of number sets are uniformly distributed. For number sets expressed in base 10, it means that the same probability holds that number will be between 10 and 100 as between 100 and 1.000. For numbers between 10 and 100, logarithm falls between 1 and 2, while for numbers between 10 and 100, logarithm falls between 2 and 3.. For some real world number sets, especially those with exponential growth over time like sales data, salaries, contracted sales values, income tax, invoices, etc. this is reasonable hypothesis.

To simplify above statements, exponential growth can be described as phenomenon of doubling in constant periods of time. For example, if certain value needs two years to double, and it has property of exponential growth, it will again double after two more years. So, value will have growth of four times at the end of fourth year, eight times at the end of sixth year etc. If certain value is started to be observed when it had value of 10 and it is doubling each two years, value will have first digit "1" throughout whole first two years. During the third and fourth year, period for next doubling, observed values will have leading digit "2" and "3" (values from 20 inclusively to 40 exclusively). Then, in fifth and sixth year, values will have leading digits "4", "5", "6" and "7". It is easy noticeable that as first digit is rising in value, larger digit values are less and less time occupying first position. Somewhere in the first half of seventh year, leading digits will pass "8" and "9". Then, values will reach 100 i.e. leading digit will become "1" again. At the end of that doubling period (end of eighth year), values will fall somewhere in range [150, 160>. It is easy noticeable that if all values (or at least representative sample) are taken from period of time spanning few doubling periods the largest probability of first digit holds for digit "1", then for digit "2", and so on, while digit "9" will have the least probability of showing on leftmost position in values. Above example shows that number sets consisting of exponentially growing values conforms to Benford's Law. However, from available literature it may be concluded that Benford's Law holds for many other cases in which exponential growth of values is not visible.

Intuitive explanation of Benford's Law is pretty clear. If company with early turnover of 10.000 kunas is observed, first digit is 1. Digit 1 will stay on first position of turnover amount until turnover rise for 100%, which is 20.000 kunas. After this, only rise of 50% is needed in order to change first digit from 2 to digit 3. It is clear that early company's

turnover will have digit 1 the most of the time because the most time is needed to change first digit from 1 to 2.

Similar explanation was offered by Nigrini in [16]: "If we think of the Dow Jones stock average as 1.000, our first digit would be 1. To get to a Dow Jones average with a first digit of 2, the average must increase to 2.000, and getting from 1.000 to 2.000 is a 100 percent increase.
Let's say that the Dow goes up at a rate of about 20 percent a year. That means that it would take five years to get from 1 to 2 as a first digit. But suppose we start with a first digit 5. It only requires a 20 percent increase to get from 5.000 to 6.000, and that is achieved in one year.

When the Dow reaches 9.000, it takes only an 11 percent increase and just seven months to reach the 10.000 mark, which starts with the number 1. At that point you start over with the first digit a 1, once again. Once again, you must double the number (10.000 to 20.000) before reaching 2 as the first digit.

As you can see, the number 1 predominates at every step of the progression, as it does in logarithmic sequences."

6.3 Properties of Conformance of Number Set to Benford's Law

In order for Benford's Law to be valid for a number set, data when sorted must form geometric sequence. Interesting example of a set that conforms to Benford's Law is Fibonacci sequence. The only prerequisite for Fibonacci sequence to be in conformance is that sequence is large enough.

In [17] and [18] criteria are set for number series to conform to Benford's Law:

1. Number series must describe values of same or similar phenomenon. E.g. lake area, heights of mountains, total yearly revenue of companies, total daily turnover on stock exchange.

2. Number series should not have defined minimal and maximal values. If minimal commission on foreign currency exchange in exchange office is 3 kunas, then set of commission values will not fit to Benford's Law, because large number of commission

values will have digit 3 as a first digit. Digit 0 is allowed minimum. Also, if a maximum value is defined, number set will not follow the law. For example, personal tax deduction maximum in Croatia is 12.000 kunas. Number distribution will tend to that limit and will cause non conformance to Benford's Law because of excessive digit 1 at leftmost position.

3. Number series should not comprise of so called assigned numbers. These numbers are assigned to various phenomena instead of description, and their important attribute is that there is no sense to perform mathematical operations on these numbers. Examples are citizens' identification numbers, bank account numbers, telephone numbers, numbers on car registration plates etc.

4. This law does not apply to numbers which creation is influenced by psychological factors, like prices in supermarket or ATM cash withdrawals.

6.4 Invariance Property of Benford's Law

Very important feature of Benford's Law is invariance. If certain number set fits Benford's Law, then the set will follow the law independently on measurement unit in which it is expressed. Consequently, if all numbers in a set that conforms to Benford's Law are multiplied by a constant different from zero, then new set will also conform to the law. For example, if the law is followed by set of total yearly companies' turnover, then the law will be followed independently on currency in which turnovers are expressed. Invariance rule also holds for reciprocal number sets. For example, if the law is followed by set of prices in kunas per stock, it will hold for numbers of stocks per kuna.

In this work invariance will be tested on specific example of number set conforming to Benford's Law. Original number set consists of 50 numbers and is shown in column OV (Table 5). Original number set conforms to Benford's Law. Invariance property is tested by multiplication with a constant number. For this test, each value in original set is multiplied by constant 3,23 and results are stored in column OVMC. The aim was to check if number set after multiplication will confirm invariance i.e. if values in OVMC column will follow Benford's Law.

ordinal number	OV	OVMC

1	10,4	33,6
2	11,7	37,8
3	12,1	39,1
4	12,4	40,1
5	14,3	46,2
6	14,8	47,8
7	15,1	48,8
8	15,6	50,4
9	15,9	51,4
10	17,5	56,5
11	17,8	57,5
12	18,1	58,5
13	18,4	59,4
14	19,2	62,0
15	19,6	63,3
16	20,4	65,9
17	21,4	69,1
18	22,6	73,0
19	23,7	76,6
20	24,3	78,5
21	25,8	83,3
22	26,3	84,9
23	27,6	89,1
24	28,1	90,8
25	31,4	101,4
26	33,3	107,6
27	35,7	115,3
28	36,6	118,2
29	38,3	123,7
30	39,8	128,6
31	42,4	137,0
32	44,6	144,1
33	46,7	150,8
34	48,3	156,0
35	49,1	158,6
36	52,1	168,3
37	54,7	176,7
38	57,1	184,4
39	59,4	191,9
40	63,2	204,1
41	66,7	215,4
42	68,7	221,9
43	72,5	234,2
44	75,3	243,2

45	77,8	251,3
46	83,1	268,4
47	87,5	282,6
48	89,6	289,4
49	94,6	305,6
50	97,2	314,0

Table 5. Multiplication of number set conforming to Benford's Law by a constant

In Table 6 frequencies and probabilities for first digit in original and multiplied number set are shown.

digit	BLp	OVf	OVp	OVMCf	OVMCp
1	0,3010	15	0,3000	15	0,3000
2	0,1761	9	0,1800	9	0,1800
3	0,1249	6	0,1200	5	0,1000
4	0,0969	5	0,1000	4	0,0800
5	0,0792	4	0,0800	6	0,1200
6	0,0670	3	0,0600	4	0,0800
7	0,0580	3	0,0600	3	0,0600
8	0,0512	3	0,0600	3	0,0600
9	0,0458	2	0,0400	1	0,0200
total:		50		50	

Table 6. Frequencies and probabilities for first digits in original and multiplied number sets

Column BLp has Benford's Law probabilities for each first digit, column OVf has frequencies of each first digit in original number set, OVp has probabilities of each first digit in original number set, OVMCf denotes frequencies of each first digit in multiplied (new) number set while OVMCp has probabilities of each first digit in multiplied (new) number set.

After brief analysis it may be concluded that new number set (created after multiplication with a constant) also conforms to Benford's Law. Some differences that appear significant (for digits 5 and 9) can be justified by small number set in which minimum absolute deviations result in significant relative deviations.

In [17, pages 27-28] market values (number of stocks outstanding times market price per stock) of 4.000 companies listed on the New York Stock Exchange (NYSE) are analyzed. It is stated that list of market values in US dollars should conform to Benford's Law. Also,

if any currency conversion (e.g. from dollars to British pounds) is performed, the new list will also conform to Benford's Law. Nigrini concludes that because conversion from one currency to another merely requires multiplication by a constant, Benford's Law will hold for a new list no matter in what currency values will be expressed. Also, conclusion that can easily be made is that by performing Benford's Law tests, no deviance can be noticed if data set is multiplied by percentage. So, if someone raises values in Benford's Law conformed data set by 10% (which is in fact multiplication by a constant 1,1) new data set will not deviate in Benford's Law terms. Furtherly, it is explained that even duplications of data i.e. double appearance of each transaction in set will not cause deviation from Benford's Law. Example describing daily volumes of buying and selling transactions in National Association of Securities Dealers Automated Quotations (NASDAQ) was given. In this system, the transactions are double counted: each transaction is counted as a sale when the stock is bought into NASDAQ and again when the stock is sold to an outside buyer. Nigrini states that the daily volumes of double counted transactions conform closely to Benford's Law as well as the daily volumes of single counted transactions. This means that if original data set conforms to Benford's Law and someone performs the action of repeating whole data set (e.g. copying and pasting) that it will not cause deviation from Benford's Law. So, if such double counted number set is audited by means of Benford's Law it will not show any deviance and practically no doubling will be noticed.

6.5 The First Digit Test

The first digit test is initial Benford's Law test. It is often used only as a test of reasonableness of selected data set. That is why auditors often call it "common sense test". However, the first digit test is most often used of all Benford's Law tests explained in 4.1. It can be used for making conclusions if significant number duplications exist in certain data set as well as for detecting clusters for certain leftmost digits.

The first digit frequencies in hypothetical example of invoice totals and corresponding Benford's Law frequencies are shown in Table 7.

digit	fo	Po	fBL	PBL	D	Dc
1	4221	0,297	4.284	0,301	-0,004	-
2	2487	0,175	2.505	0,176	-0,001	-
3	1761	0,124	1.779	0,125	-0,001	-
4	1301	0,091	1.380	0,097	-0,006	-

5	1406	0,099	1.124	0,079	0,020	+
6	902	0,063	953	0,067	-0,004	-
7	812	0,057	825	0,058	-0,001	-
8	708	0,050	726	0,051	-0,001	-
9	633	0,044	655	0,046	-0,002	-
sum	14.231		14.231			

Table 7. The first digit frequencies in hypothetical example of invoice totals

The column *fo* contains counts of numbers with the first digit from column digit. For example, there were 4221 invoices with leftmost digit "1" for its total values. The sum of *fo* column equals the number of observations in the data set i.e. total number of observed invoices.

The column *Po* gives the probability (or actual proportion) that invoice total will have certain digit on its most valued position. In this example, probability of 5% is that invoice total will have digit "8" on leftmost position. Calculation is performed by dividing values in *fo* column (actual counts) with total number of observed invoices.

The column *fBL* has the expected frequencies of Benford's Law for first digits. Expected Benford's Law frequencies are calculated by multiplication of Benford's Law expected probabilities (column *PBL*) and actual frequencies (column *fo*).

The column *PBL* has the expected probabilities of Benford's Law for first digits. Numbers in this column are calculated from expression (1) in chapter 5.1.

The column *D* has values of actual probabilities deviation from Benford's Law probabilities. It is calculated as difference between columns *Po* and *PBL*. Values above zero denotes positive deviations which means that there are more numbers with certain first digit in actual data set than it is expected by Benford's Law. Values below zero highlight that certain digit has lesser count in observed data set than expected by Benford's Law.

Consequently, the column *Dc* shows the direction of deviation. The "+" sign denotes positive deviation (only for digit "5") while the "-" indicates negative deviations. Positive deviation means that frequency for certain digit is greater than corresponding Benford's Law frequency, while negative deviation means frequency is smaller than related Benford's Law frequency.

Figure 1 shows first digit probabilities of actual hypothetical data set and Benford's Law probabilities.

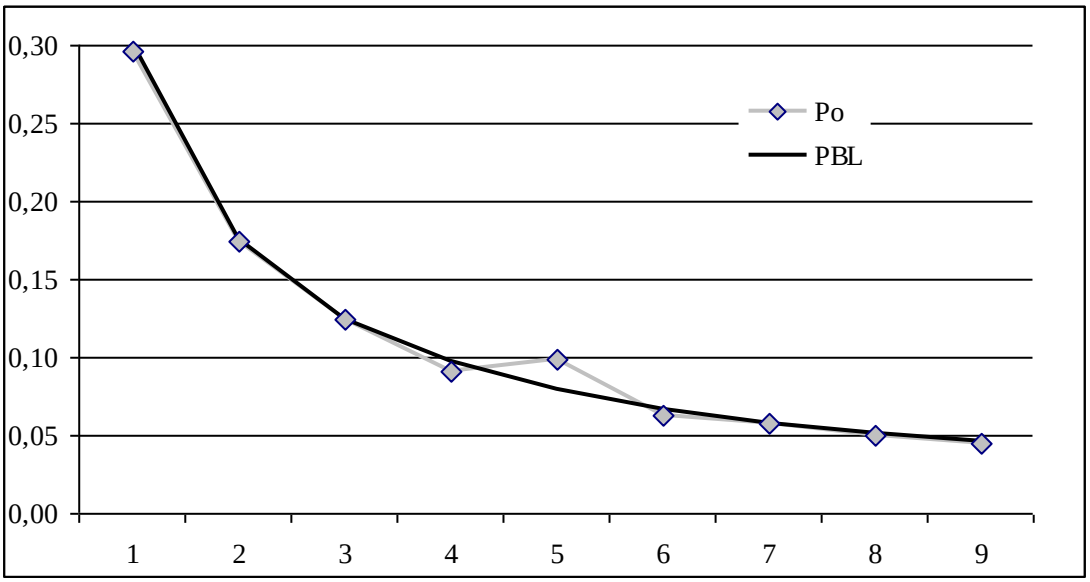

Figure 1. First digit probabilities of actual data set and Benford's Law probabilities

Based on a visual analysis of this graph it could be stated that chosen data set of invoice totals are following the Benford's Law. However, from auditors' perspective, the digit "5" should be a matter of further analysis. The digit "5" has the only, conditionally said, significant spike on the graph. This spike is resulting from positive deviation of 0,02 in absolute value which corresponds to 25% in relative value. This may be a consequence of mistakes, flaws or even fraudulent activity. Of course, there may be a logical explanation for such deviation resulting from business internal processes or influences from business environment. In this case, further analysis that should be performed are the first two digits test, the first three digits tests, number rounding and number duplication tests. These tests could proof or deny existence of deviations resulting from inadequate business processes and controls.

The first digit Benford's Law test can not be a final proof that data is erroneous, fraudulent or flawed, nor that some irregular activities has taken place. Some more detailed and focused tests, together with analysis of business processes and rule, must be undertaken. However, the first digit Benford's Law test may be a first warning that some additional audit actions should be performed.

Of course, there is a certain need to define conformance criteria i.e. to define when some number set conforms to Benford's Law and when it is not the case. Visual inspection can

not be a valid judgment. Certainly, judgment by the auditors "feeling about the numbers" is also not appropriate. Some statistical tests should be performed in order to test if actual number set conforms to Benford's Law. In this paper statistical tests used for conformance measurement are Z-statistics, Mean Average Deviation and Chi-square. These tests are explained in more details in chapter 6.9.

6.6 The First Two Digits Test

The first two digits test has much more audit relevance than the first digit test. It is more focused since it takes into account 90 combinations of the first two left most digits. After performing this test, auditor can spot finer irregularities or discrepancies and then perform additional analysis.

The first two digits of a number are the first two most valued digits, e.g. in number 543, digits "5" and "4" are the first and second digits respectively. As it can be easily noticed, there are 90 possible combinations of the first two digits (from "10" to "99").

Another hypothetical example of invoice total amounts is shown in Table 8.

digits	fo	Po	fBL	PBL	D	Dc
10	7.767	0,04234	7.594	0,04139	0,00094	+
11	6.855	0,03737	6.933	0,03779	-0,00042	-
12	6.311	0,03440	6.377	0,03476	-0,00036	-
13	6.002	0,03272	5.905	0,03218	0,00053	+
14	5.398	0,02942	5.497	0,02996	-0,00054	-
15	5.178	0,02822	5.142	0,02803	0,00020	+
16	4.712	0,02568	4.830	0,02633	-0,00064	-
17	4.465	0,02434	4.554	0,02482	-0,00049	-
18	4.367	0,02380	4.308	0,02348	0,00032	+
19	4.096	0,02233	4.087	0,02228	0,00005	+
20	3.955	0,02156	3.887	0,02119	0,00037	+
21	3.675	0,02003	3.706	0,02020	-0,00017	-
22	3.447	0,01879	3.542	0,01931	-0,00052	-
23	3.273	0,01784	3.391	0,01848	-0,00064	-
24	3.244	0,01768	3.253	0,01773	-0,00005	-
25	3.230	0,01761	3.125	0,01703	0,00057	+
26	2.945	0,01605	3.007	0,01639	-0,00034	-
27	3.245	0,01769	2.898	0,01579	0,00189	+
28	3.888	0,02119	2.796	0,01524	0,00595	+
29	4.264	0,02324	2.701	0,01472	0,00852	+
30	2.221	0,01211	2.613	0,01424	-0,00213	-
31	2.378	0,01296	2.530	0,01379	-0,00083	-

32	2.331	0,01271	2.452	0,01336	-0,00066	-
33	2.333	0,01272	2.379	0,01296	-0,00025	-
34	2.276	0,01241	2.310	0,01259	-0,00018	-
35	2.305	0,01256	2.245	0,01223	0,00033	+
36	2.124	0,01158	2.183	0,01190	-0,00032	-
37	2.087	0,01138	2.125	0,01158	-0,00021	-
38	1.987	0,01083	2.070	0,01128	-0,00045	-
39	1.974	0,01076	2.017	0,01100	-0,00024	-
40	2.087	0,01138	1.967	0,01072	0,00065	+
41	1.889	0,01030	1.920	0,01047	-0,00017	-
42	1.854	0,01011	1.875	0,01022	-0,00011	-
43	1.765	0,00962	1.832	0,00998	-0,00036	-
44	1.755	0,00957	1.791	0,00976	-0,00019	-
45	1.807	0,00985	1.751	0,00955	0,00030	+
46	1.669	0,00910	1.714	0,00934	-0,00024	-
47	1.665	0,00908	1.677	0,00914	-0,00007	-
48	1.633	0,00890	1.643	0,00895	-0,00005	-
49	1.598	0,00871	1.610	0,00877	-0,00006	-
50	1.556	0,00848	1.578	0,00860	-0,00012	-
51	1.532	0,00835	1.547	0,00843	-0,00008	-
52	1.489	0,00812	1.518	0,00827	-0,00016	-
53	1.423	0,00776	1.489	0,00812	-0,00036	-
54	1.412	0,00770	1.462	0,00797	-0,00027	-
55	1.445	0,00788	1.436	0,00783	0,00005	+
56	1.311	0,00715	1.410	0,00769	-0,00054	-
57	1.156	0,00630	1.386	0,00755	-0,00125	-
58	965	0,00526	1.362	0,00742	-0,00216	-
59	929	0,00506	1.339	0,00730	-0,00224	-
60	1.301	0,00709	1.317	0,00718	-0,00009	-
61	1.277	0,00696	1.296	0,00706	-0,00010	-
62	1.245	0,00679	1.275	0,00695	-0,00016	-
63	1.252	0,00682	1.255	0,00684	-0,00002	-
64	1.213	0,00661	1.235	0,00673	-0,00012	-
65	1.199	0,00654	1.216	0,00663	-0,00010	-
66	1.188	0,00648	1.198	0,00653	-0,00006	-
67	1.174	0,00640	1.180	0,00643	-0,00003	-
68	1.154	0,00629	1.163	0,00634	-0,00005	-
69	1.102	0,00601	1.146	0,00625	-0,00024	-
70	1.166	0,00636	1.130	0,00616	0,00020	+
71	1.076	0,00587	1.114	0,00607	-0,00021	-
72	1.081	0,00589	1.099	0,00599	-0,00010	-
73	1.056	0,00576	1.084	0,00591	-0,00015	-
74	1.033	0,00563	1.069	0,00583	-0,00020	-
75	1.064	0,00580	1.055	0,00575	0,00005	+
76	1.022	0,00557	1.042	0,00568	-0,00011	-
77	1.001	0,00546	1.028	0,00560	-0,00015	-
78	976	0,00532	1.015	0,00553	-0,00021	-

79	988	0,00539	1.002	0,00546	-0,00008	-
80	977	0,00533	990	0,00540	-0,00007	-
81	966	0,00527	978	0,00533	-0,00006	-
82	952	0,00519	966	0,00526	-0,00008	-
83	924	0,00504	954	0,00520	-0,00016	-
84	926	0,00505	943	0,00514	-0,00009	-
85	909	0,00495	932	0,00508	-0,00012	-
86	908	0,00495	921	0,00502	-0,00007	-
87	901	0,00491	911	0,00496	-0,00005	-
88	897	0,00489	900	0,00491	-0,00002	-
89	892	0,00486	890	0,00485	0,00001	+
90	901	0,00491	880	0,00480	0,00011	+
91	853	0,00465	871	0,00475	-0,00010	-
92	855	0,00466	861	0,00470	-0,00003	-
93	851	0,00464	852	0,00464	-0,00001	-
94	838	0,00457	843	0,00460	-0,00003	-
95	835	0,00455	834	0,00455	0,00000	+
96	820	0,00447	826	0,00450	-0,00003	-
97	807	0,00440	817	0,00445	-0,00006	-
98	802	0,00437	809	0,00441	-0,00004	-
99	804	0,00438	801	0,00436	0,00002	+
Total:	183.459		183.459			

Table 8. The first two digit frequencies of invoice total amounts (hypothetical example)

The column *fo* has total number of occurrences of first two digits from column *digit*. For example, in observed data set, there were 6876 occurrences of first two leftmost digits "11". The sum of *fo* column equals the total number of observations in the data set i.e. total number of observed invoices.

The column *Po* contains the probabilities (or actual proportions) that invoice total amounts will have certain first two digits indicated in column *digit* on its leftmost positions. For example, actual proportion of digit "14" on leftmost position of invoice amounts is 0,02979 or 2,9%. Calculation is done by dividing values in column *fo* (actual occurrences) by total number of observed invoices (183.459).

The column *fBL* contains the expected frequencies of Benford's Law for first two digits in column *digit*. Expected frequencies according to Benford's Law are calculated by multiplying Benford's Law expected probabilities (column *PBL*) and actual frequencies (column *fo*).

The column *PBL* includes the expected probabilities of Benford's Law for first two digits. Values in this column are calculated from expression:

$PBL(z_1z_2)=\log_{10}(1+1/z_1z_2)$, $z_1z_2 \in [10..99]$

where z_1 denotes first (leftmost) digit and z_2 second digit. Since decade number system is observed, logarithms with base 10 are taken into account.

The column D has values of actual probabilities deviation from Benford's Law probabilities and it is calculated as difference between columns Po and PBL. Positive values in this column signify that there are more numbers with certain first two digits in observed data set than it could be expected by Benford's Law. Negative values in this column indicate that certain first two digits have lesser count in observed data set than expected by Benford's Law.

Accordingly, the column Dc shows the direction of deviation. The "+" sign denotes positive deviation while the "-" indicates negative deviations. Positive deviation means that frequency for certain digit is greater than corresponding Benford's Law frequency, while negative deviation means frequency is smaller than related Benford's Law frequency.

Figure 2 shows first two digits probabilities of observed hypothetical data set and Benford's Law probabilities.

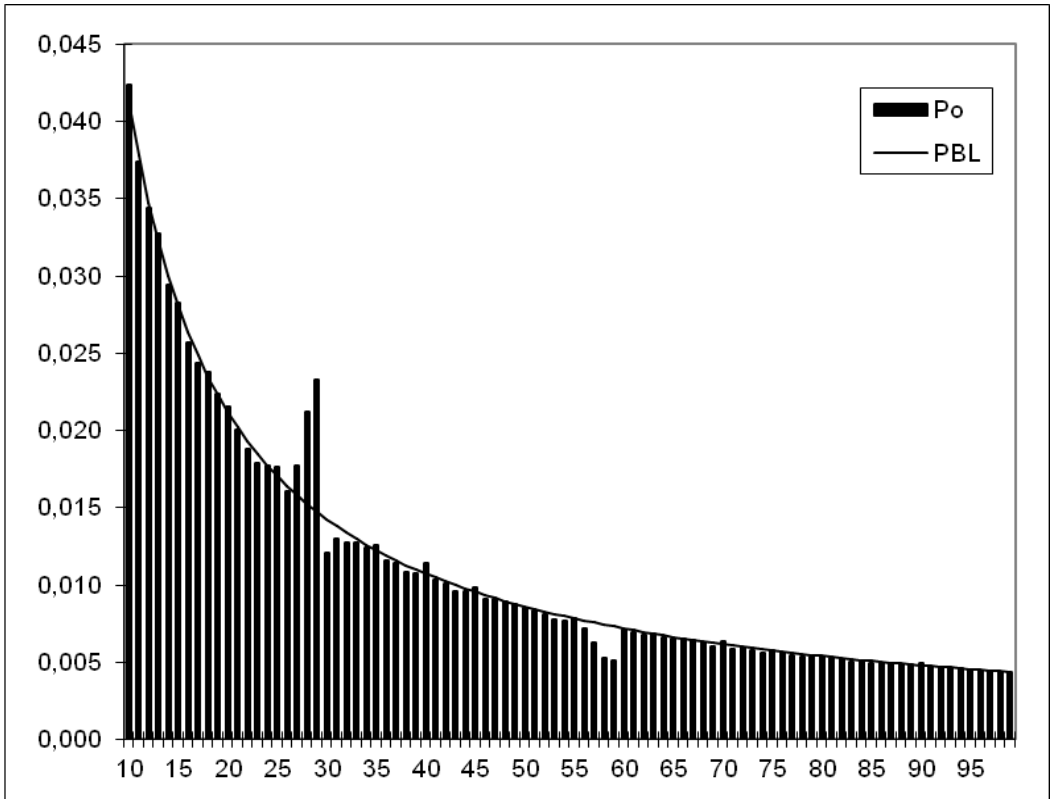

Figure 2. First two digits probabilities of observed hypothetical data set (Po) and Benford's Law probabilities (PBL)

Based on a visual analysis of this graph it could be stated that chosen data set of invoice total amounts are following the Benford's Law for majority of first two digits. However, auditors can easily spot significant positive spikes on first two digits in interval [27..29]. These digits have the only, conditionally said, significant spikes on the graph. Spikes are resulting from positive deviations of 0,00189 in absolute value for digits "27" to 0,00852 in absolute value for digits "29". Also, it is noticed that there are significant shortages of first two digits within set [30..32] and set [56..59].

Digits	D	Dc	PCd
27	0,00189	+	11,99
28	0,00595	+	39,06
29	0,00852	+	57,86
30	-0,00213	-	-14,99
31	-0,00083	-	-5,99
32	-0,00066	-	-4,92
56	-0,00054	-	-7,04
57	-0,00125	-	-16,58
58	-0,00216	-	-29,15
59	-0,00224	-	-30,63

Table 9. Focus on digits with excessive frequencies

In addition to Table 8, column PCd appears in table 9. It holds percentages of deviation between actual and expected frequencies. It means that, for example, there is 11,99% more total invoice amounts with first two digits "27" than it could be expected by Benford's Law. Also, as spikes and values in PCd column show, there are excesses in frequencies for first two digits “28” and “29”. Additionally, as it is shown in Table 9, there are significant deficits of first two digits within sets [30..32] and [56..59].

During the audit activity, these positive, excessive frequencies listed in Table 9 must be in the focus of auditor’s interest. Digits with excessive frequencies hold numbers with excessive duplications or clustering around specific limits.

This may be a consequence of mistakes, flaws or even fraudulent activity. Of course, there may exist a logical explanation that these deviations result from business internal rules or some influences from business environment. However, to make appropriate conclusion

further analysis may be performed like the first three digits tests, number rounding and number duplication tests. These tests could proof or deny that deviations result from inadequate business processes and controls. Also, it is important to understand business rules established within certain business process in company being audited.

In our example, auditor may have discovered that there are certain rules established in company whose received invoices are examined. One of the rules may have stated that all invoices with total amounts above 3.000 kunas are subject to manager's approval for payment. All invoices with total amounts less than 3.000 kunas require only co-signature by two financial department employees in charge of issuing payments. In Table 9 it is visible that there is significant surplus of invoices with first two numbers between "27" and "29". It may be assessed personnel was trying to avoid 3.000 limit by negotiating invoices slightly bellow it. Also, it is suspicious that there is lack of first two digits between "30" and "32". It may be a consequence of negotiating total amounts bellow 3.000 with supplier in order to avoid manager's approval. In addition, there is significant shortage of first two digits between "56" and "59". This may be a lead that personnel negotiated splitting of invoices in two with supplier. By splitting invoices between 5.600 and 6.000 (excluding) in two invoices with total amounts less than 3.000, the necessity for manager's approval will again be averted. So, additional examination should be performed in order to check if significant number of invoices with total amounts between 2.700 and 3.000 exist. After this simple test is performed, auditor can confirm or deny his doubts. Also, auditor my check if authorization of invoices with total amounts between 2.700 and 3.000 is usually performed by same pair(s) of employees. If at the same time there is significant lack of authorizations done by these pair(s) of employees for amounts between 3.000 and 3.300, as well between 5.600 and 6.000 kunas then it may be important fact which rises possibility of fraud commitment.

Similarly as for the first digit test, the first two digits Benford's Law test can not be a final proof that data is erroneous, fraudulent or flawed, nor that some irregular activities has taken place. More focused tests, together with analysis of business rules must be executed. Although, the first two digits Benford's Law test is much more focused than the first digit test and it significantly narrows audit scope. The result of that narrowing is easier selection of audit targets which should be furtherly investigated. Auditors may use the first two digits test as a logical extension of the first digit test, as well as the second digit test.

Of course, there is a certain need to define conformance criteria i.e. to define when some number set conforms to the first two digits Benford's Law test. As with the first digit test, visual inspection can not be a valid judgment in auditing procedure. More on some statistical tests that should be performed in order to test if actual number set conforms to Benford's Law can be found in chapter 6.9.

6.7 The First Three Digits Test

Corporate data sets that are in focus of auditor are growing larger and larger. Extremely large data sets are usually quite demanding and not adequate for effective audit. That is the consequence of too large scope and focus being not detailed enough. Although the first two digits test may significantly improve focus of audit and very often enables creation of adequate audit targets, sometimes data subsets of the first two digits are too large and no significant deviation can be spotted. However, as it is stated in chapter 5.1, Benford's Law can be applied to any digit in number and also to first n digits in number set. So, the first two digits test can be furtherly adjusted to the first three digits test in order to preserve data set sizes auditable.

Smaller subset tests like the first three digits test create smaller data sets with possibly more significant irregularities, assuring that data audit become more manageable. There are 900 possible combinations of the first three digits i.e. all integers in set [100..999]. The first three digits that are observed are in fact three leftmost digits in numbers i.e. three most valued digits. As with previous two tests, eventually leading zeros should be omitted from analysis. For example, in the number "2381" the first three digits are "238". Also, in the number "47", the first three digits are "470" since number "47" can be represented as "47,00".

Since there are 900 possible first three digits combinations and only 90 possible first two digits combinations, it is obvious that the first three digits test will be much more focused than the first two digits test. The first three digits test will give to auditor significantly smaller data sets which are much more adequate for audit. In this paper (chapter 6.6), it is noticed and explained that the first two digits test can find out irregularities based on evading certain limits or thresholds if clustering is based on the first two digits. However, if clustering is not significant on the first two digits but on the first three digits, then only

the first three digits test can notice such clusters i.e. duplications of certain first three digits.

Lets introduce hypothetical example in which auditor is examining invoices received from suppliers that were or about to be paid (accounts payable data) and that auditor performed the first two digits test. Auditor is especially focused on invoices amounts around 5.000 kunas. Management defined specific rule for payment authorization: all amounts above 5.000 kunas must be authorized by financial department manager while invoices with lesser amounts have to be authorized only by two employees of the operating level. Part of the first two digits test, that was in auditor's focus because of specific authorization rule, is shown in Table 10:

digits	fo	Po	fBL	PBL	D	Dc	PCd
...	...	...	...	...	...	...	...
48	611	0,00909	602	0,00895	0,00013	+	1,50
49	583	0,00867	590	0,00877	-0,00010	-	-1,19
50	556	0,00827	578	0,00860	-0,00033	-	-3,81
51	558	0,00830	567	0,00843	-0,00013	-	-1,59
52	559	0,00831	556	0,00827	0,00004	+	0,54
...	...	...	...	...	...	...	...
total:	67234		67234				

Table 10. The first two digits test for received invoices

Explanation of columns in Table 10 (digits, fo, Po, fBL, PBL, D, Dc, PCd) it the same as for these columns in Table 8 and Table 9 in chapter 6.6. In table 10 only first two digits that are close to "50" threshold are examined. Assumption was set that significant excessive counts for digits "48" and especially "49" will be found. However, after the first two digits test, auditor may conclude that there are no significant surpluses of numbers with first two digits "48" and "49". On the contrary, frequency of digits "49" is even smaller than expected by Benford's Law. There is 1,19% shortage of numbers starting with "49" (7 less in absolute value). Values starting with "48" are in slight, insignificant surplus. Only first digit combination "50" has discrepancy that earns attention – it is deficient for 3,81%.

There is no significant negative bias for numbers starting with digits "51" and "52". Auditor could conclude that data conform to Benford's Law since there are no significant

positive spikes on graph shown on Figure 3 which is based on actual (Po) and Benford's Law (PBL) proportions.

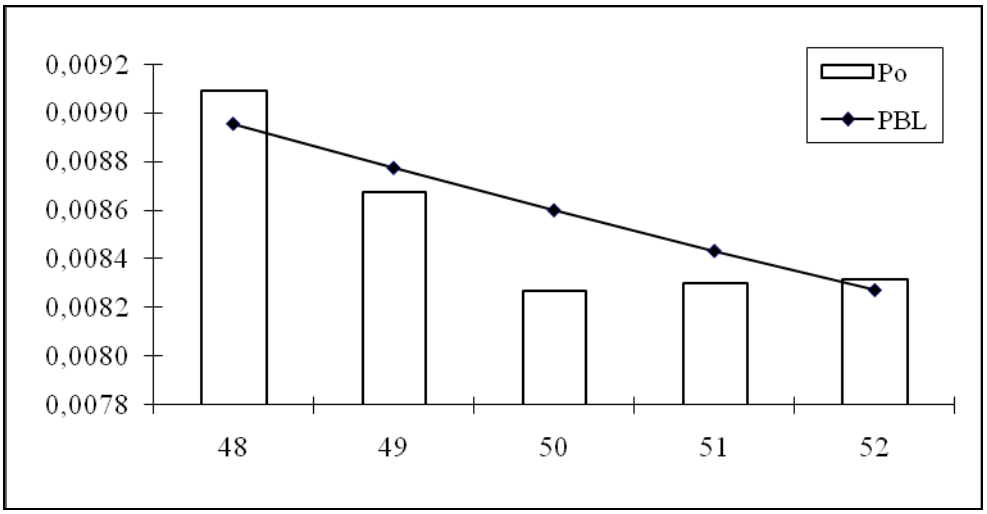

Figure 3. First two digits - actual (Po) and Benford's Law (PBL) proportions

However, with the first three digits test, it is possible to disclose much more cases of fraud, mistakes or evasion than with the first two and especially the first digit tests. In Table 11 excerpt from table of the first three digits test is shown. Only digit combinations that follow from the first two digits combinations from Table 10 are analysed.

digits	fo	Po	fBL	PBL	D	Dc	PCd
...	...	...	...	...	...	...	...
480	63	0,00094	61	0,00090	0,00003	+	3,28
481	61	0,00091	61	0,00090	0,00001	+	0,00
482	62	0,00092	61	0,00090	0,00002	+	1,64
483	61	0,00091	60	0,00090	0,00001	+	1,67
484	59	0,00088	60	0,00090	-0,00002	-	-1,67
485	58	0,00086	60	0,00089	-0,00003	-	-3,33
486	61	0,00091	60	0,00089	0,00001	+	1,67
487	61	0,00091	60	0,00089	0,00002	+	1,67
488	63	0,00094	60	0,00089	0,00005	+	5,00
489	62	0,00092	60	0,00089	0,00003	+	3,33
490	53	0,00079	60	0,00089	-0,00010	-	-11,67
491	52	0,00077	59	0,00088	-0,00011	-	-11,86
492	54	0,00080	59	0,00088	-0,00008	-	-8,47
493	53	0,00079	59	0,00088	-0,00009	-	-10,17
494	53	0,00079	59	0,00088	-0,00009	-	-10,17
495	53	0,00079	59	0,00088	-0,00009	-	-10,17
496	54	0,00080	59	0,00087	-0,00007	-	-8,47

497	66	0,00098	59	0,00087	0,00011	+	11,86
498	71	0,00106	59	0,00087	0,00018	+	20,34
499	74	0,00110	58	0,00087	0,00023	+	27,59
500	32	0,00048	58	0,00087	-0,00039	-	-44,83
501	42	0,00062	58	0,00087	-0,00024	-	-27,59
502	47	0,00070	58	0,00086	-0,00017	-	-18,97
503	47	0,00070	58	0,00086	-0,00016	-	-18,97
504	66	0,00098	58	0,00086	0,00012	+	13,79
505	65	0,00097	58	0,00086	0,00011	+	12,07
506	65	0,00097	58	0,00086	0,00011	+	12,07
507	64	0,00095	58	0,00086	0,00010	+	10,34
508	64	0,00095	57	0,00085	0,00010	+	12,28
509	64	0,00095	57	0,00085	0,00010	+	12,28
510	59	0,00088	57	0,00085	0,00003	+	3,51
511	55	0,00082	57	0,00085	-0,00003	-	-3,51
512	54	0,00080	57	0,00085	-0,00004	-	-5,26
513	55	0,00082	57	0,00085	-0,00003	-	-3,51
514	55	0,00082	57	0,00084	-0,00003	-	-3,51
515	56	0,00083	57	0,00084	-0,00001	-	-1,75
516	54	0,00080	57	0,00084	-0,00004	-	-5,26
517	58	0,00086	56	0,00084	0,00002	+	3,57
518	56	0,00083	56	0,00084	0,00000	-	0,00
519	56	0,00083	56	0,00084	0,00000	-	0,00
520	59	0,00088	56	0,00083	0,00004	+	5,36
521	56	0,00083	56	0,00083	0,00000	+	0,00
522	55	0,00082	56	0,00083	-0,00001	-	-1,79
523	54	0,00080	56	0,00083	-0,00003	-	-3,57
524	57	0,00085	56	0,00083	0,00002	+	1,79
525	53	0,00079	56	0,00083	-0,00004	-	-5,36
526	57	0,00085	55	0,00082	0,00002	+	3,64
527	56	0,00083	55	0,00082	0,00001	+	1,82
528	55	0,00082	55	0,00082	0,00000	-	0,00
529	57	0,00085	55	0,00082	0,00003	+	3,64
...	...	...	...	...	...	...	...

Table 11. First three digits combinations that follow from first two digits combinations from Table 10

A few significant deviations can be spotted in Table 11. Positive differences between actual and Benford's Law frequencies can easily be noticed for first three digits "498" and "499". On the contrary, there is lack of first three digits "500", "501", "502" and "503".

Positive spikes and corresponding sinks are visible on Figure 4.

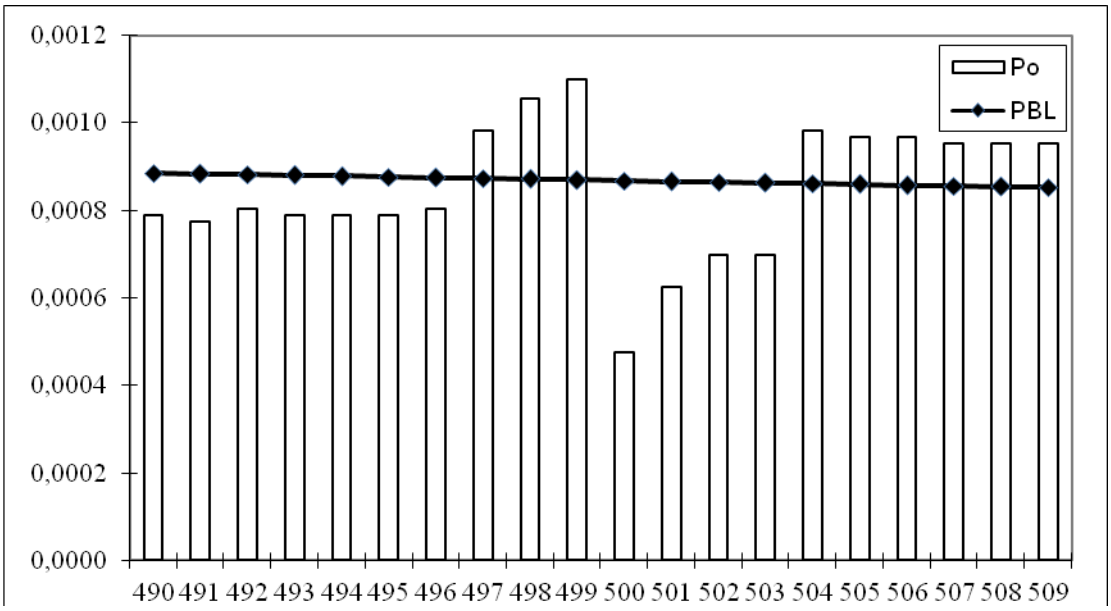

Figure 4. First three digits - "Spikes" and "sinks"

From the above Table 11 and Figure 4 auditor may judge that operating personnel dealing with invoice authorization and payment was trying to avoid 5.000 limit. Additional argument for such judgment is a lack of numbers starting with digits "500", "501", "502" and "503". Sinks for these three digits combinations are clearly visible on a Figure 4. Shortages are ranging from 44% (for digits "500") to 19% (for digits "502" and "503"). From an auditor's perspective, it is very significant that shortages are the greatest for digits "500", and lesser toward digits "503". Auditor may assess that reason for such distribution is fabrication of invoices slightly greater than 5.000 (e.g. between 5.000 and 5.040 exclusively). Fraudsters probably estimated it is less risky and less obvious if certain invoice amount is updated for a small amount. Also, there is a lesser "loss" for supplying company if amount is changed only for small figure. So, there is a certain probability that these invoice amounts are reduced in order to fall bellow 5.000 limit. Avoidance of limit could be done in arrangement with certain suppliers. Operating personnel could agree with some supplier(s) that invoices fall slightly bellow 5.000 limit in order to avoid additional check and payment authorization by manager. That way, even payments without received goods or services could be transacted. Motivation for such transactions on supplier side is obvious: supplying company rises its revenue and supplier salesman rises his bonus amount. Besides, supplying company eventually loose insignificant amount of money for delivered goods and services by reducing invoices for few kunas. Of course, for eventually paid undelivered goods and services supplying company earns full invoice amount. What

is yet missing here is only motivation of operating personnel in impaired company. Operating personnel might make a deal with supplying company to receive allowance for fraudulent paid invoices. So, motivation for fraudulent activity is clear for both participating parties.

Additional audit activity may include checks if authorization of invoices with amounts between 4.800 and 5.000 kunas is performed usually by the same pair(s) of operating employees. Auditor should analyse authorizations of payments for invoices between 5.000 and 5.040 exclusively. If there is a significant lack of authorizations done by before mentioned pair(s) of operating personnel, then it is important proof that fraudulent activity is on stage. Auditor should also check how often certain suppliers are issuing invoices just bellow 5.000 kunas. If certain supplier has more than average occurrence in observed set of invoices, then it may be a lead that supplier agreed actions with operating personnel.

6.8 The Second Digit Test

Similarly to the first digit test, the second digit test may be used in auditing context as a check of data on reasonableness. Since there are only 10 combinations of second digits (0-9), audit data subsets are too large for carrying out detailed auditing activity. Nevertheless, with second digit test it may be possible to make valuable conclusions about existence of number clustering or considerable number duplications.

The example of the second digit test will be executed on hypothetical data set of insurance sales. Let us assume that life insurance company has a certain rules for bonuses calculation of insurance salesmen:

- for contracted insurance policies with yearly premium bellow 5.000 kunas, bonus percentage is 1%
- for contracted insurance policies with yearly premium between 5.000 and 15.000 kunas, bonus percentage is 2%
- for contracted insurance policies with yearly premium above 15.000 kunas, bonus percentage is 3%

Let us suppose that auditor gathered data about yearly policies and that he performed the second digit test with outcome represented in Table 12.

digit	fo	Po	fBL	PBL	D	Dc	PCd
0	2.356	0,12859	2.193	0,11968	0,009	+	7,43
1	2.213	0,12078	2.087	0,11389	0,007	+	6,04
2	2.002	0,10927	1.994	0,10882	0,000	+	0,40
3	1.887	0,10299	1.912	0,10433	-0,001	-	-1,31
4	1.778	0,09704	1.838	0,10031	-0,003	-	-3,26
5	1.839	0,10037	1.771	0,09668	0,004	+	3,84
6	1.698	0,09268	1.711	0,09337	-0,001	-	-0,76
7	1.645	0,08978	1.655	0,09035	-0,001	-	-0,60
8	1.541	0,08411	1.604	0,08757	-0,003	-	-3,93
9	1.373	0,07494	1.557	0,08500	-0,010	-	-11,82
total	18.322		18.322				

Table 12. The second digit frequencies in contracted yearly insurance policies

In Table 12, a few deviations are easily noticeable. Firstly, there are surpluses of the second digits 0, 1 and 5. Secondly, there are shortages of digits 4, 8 and 9.

Positive surpluses and negative shortages are shown in Figure 5.

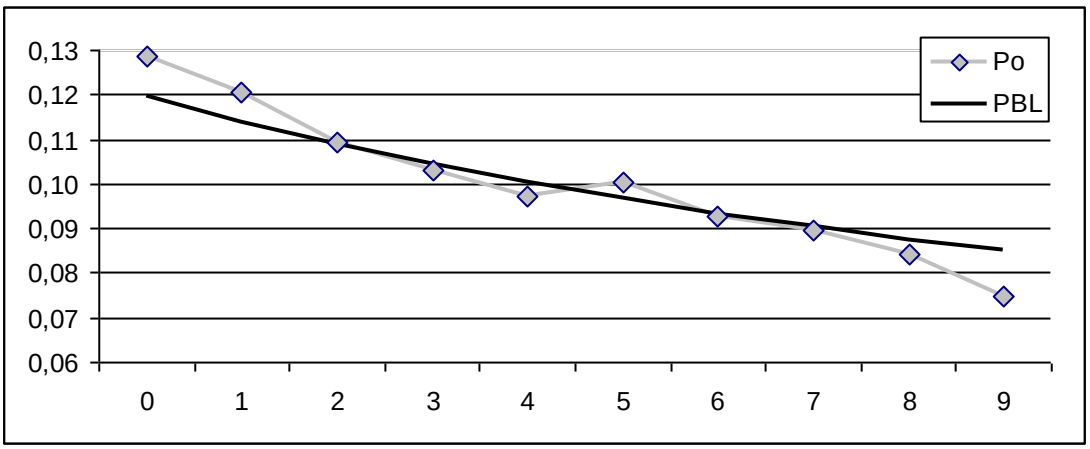

Figure 5. The second digit frequencies

Based on a visual analysis of Figure 5 graph it could be stated that chosen data set of yearly insurance policies have significant positive deviations for the second digits "0" (excess of 7,43% from Benford's Law frequency) and "1" (excess of 6,04% from Benford's Law frequency). Also, there can be clearly seen that second digit "4" has shortage (-3,26% from Benford's Law frequency) and second digit "5" has positive spike (excess of 3,84% from Benford's Law). Auditor should learn more about rules for insurance salesman bonuses. Three rules explained shortly on page 78 set two limit boundaries. First boundary

is set to amount of 5.000 kunas and second to amount of 15.000 kunas. These boundaries have second digits "0" and "5" respectively. Rules define progressive bonus percentages according to rise in amount of contracted yearly premium. It can be suspected that on each boundary there are deviations from the Benford's Law second digit test. Surpluses are evident on second digits which may correspond to amounts just above the rule boundaries. According to excessive counts, auditor may suppose there are surpluses of yearly premiums with amounts just above bonus limits (5.000 and 15.000). As a consequence, there is lack of digit "9" (-11,82%) and digit "8" (-3,93%) as a second digit. The greatest excess of second digit is for digit "0" so auditor may assume insurance salesmen are pushing insurance contracts just above 5.000 limit in order to skip corresponding bonuses to next level (2%). The same assumption can be done for shortages of second digits "8" and "9". Salesmen are pushing contracted insurance premiums from values close to boundary (from 4.800 to 5.000 exclusively) to values just over the boundary (5.000) and that is the reason for shortage in digits "8" and "9". Auditor may also understand this is done because salesmen are trying to pump their bonuses. The same may be assumed for excessive count of second digit "5": salesmen are pushing values between 14.000 to 15.000 (exclusively) over 15.000 boundary in order to gain 3% bonus instead of 2%. Of course, if skipping over defined limits is confirmed by actual business event and these amounts freely chosen by policy holder, then there is no proof for fraudulent activity.

Since the second digit test is too broad and has too large auditing sample, it is not possible to make final judgement exclusively by this test. Assumptions can be confirmed only after numbers are closely analysed. For example, if auditor additionally performed the first two digits test, he may get results that are denying previous, too early set, assumptions. The first two digits test could shown that excesses in second digits "0", "1" and "5" are results of excessive number of policies valued between 7.000 and 7.200 (exclusively) and between 3.500 and 3.600 (exclusively). And reason for such discrepancies may be also very pragmatic and consequence of a state tax policy if tax relief boundaries are set on 3.500 and 7.000 values.

6.9 Benford's Law Conformance Criteria

In chapters 6.1, 6.2, 6.3 and 6.4 are defined and explained some properties of Benford's Law. In chapters 6.5, 6.6, 6.7 and 6.8 certain Benford's Law tests are explained and possible audit scenarios are developed.

In a few examples it is shown how auditors may react on results of Benford's Law tests even without any specific statistical measure of deviation, apart from calculation of percentage deviation. Simple percentage of deviation measurement and visual inspection of graph results were suitable for making some important evaluations about number sets. Of course, these evaluations were matter of further analysis which was based on additional Benford's Law tests, analysis of business process rules, furtherly narrowing data set in order to get smaller audit set which is more suitable for auditing and making final conclusion. In usual auditing environment, Benford's Law tests are not used as a final proof of misconduct, omissions, fraud or inappropriateness of business process. After auditor realized that there are significant deviations in comparison to Benford's Law, usually additional investigation must be performed. That is why conformance criteria to Benford's Law in auditing environment are not of a crucial importance.

However, although visual inspection of graphs shown in previous examples as well as simple percentage deviation calculus can be very often satisfactory in auditing environment, it is desirable to define certain conformance criteria. Conformance criteria should give clear answer if data set conforms to Benford's Law or not. In fact, conformance criteria should with certain probability answer a question whether data set follows the Benford's Law. Some conformance criteria also give the probability that non-conformance is consequence of a chance alone.

For purposes of conformance measurement of data set concerning Benford's Law tests, statistical methods like Z-statistics, Chi square and Mean Absolute Deviation will be explained and used in data analysis.

6.9.1 Z-statistics

Z-statistics is used as measure of statistical significance of deviation from Benford's Law for each digit combination separately. It uses expected and actual probabilities as well as total number of observations. Z-statistics can be calculated from formula:

$$Z = \frac{\left|Po - PBL\right| - \frac{1}{2n}}{\sqrt{PBL(1-PBL)\frac{1}{n}}}$$

In this formula, Po denotes the observed (actual) proportion, PBL is expected Benford's Law proportion, n is total number of observations. The term $\frac{1}{2n}$ is correction factor which is used only if it is smaller than term $\left|Po - PBL\right|$.

In fact, the Z-statistics measures if deviation of observed (actual) proportion from the expected (Benford's Law) proportion is statistically significant or not. Larger the Z-statistics for certain digit(s) the larger is probability that deviations are not accidental. Auditor may choose and set limiting Z-statistics value according to his acceptable level of accidental deviations. If the auditor decided he will accept only 1% of chance to make wrong conclusions, then he would define maximum Z-statistics of 2,58. If certain Z-statistics is larger than 2,58, then it may be concluded that there is only 1% probability that significant deviation from expected frequency is result of a chance. So, if Z-statistics is larger than 2,58 auditor may conclude that probability of fraud, omissions or errors is quite high for observed data subset. So, in the cases of the Benford's Law first digit test, Z-statistics for each of 9 digits should be calculated. All Z-statistics larger than previously set limit level (e.g. 2,58 for 1% error level) should be marked as suspicious. Those digits should be furtherly investigated in order to check if deviations are result of frauds, errors or omissions or deviations are only consequences of a chance or business rules.

In addition to 1% limit level (i.e. Z-statistics of 2,58), auditors may choose other maximum allowable Z-statistics. For example, if auditor wants to accept only 5% significance level which means there is only 5% probability that difference between actual and expected frequency values is accidental, he will set Z-statistics to 1,96 value. It is said that cut off value for each Z-statistics value is 1,96. All values that exceed this value should be flagged

as they deviate according to Z-statistics. Graphical illustration of normal curve and corresponding cut off values for 1% and 5% significance levels is shown on Figure 6.

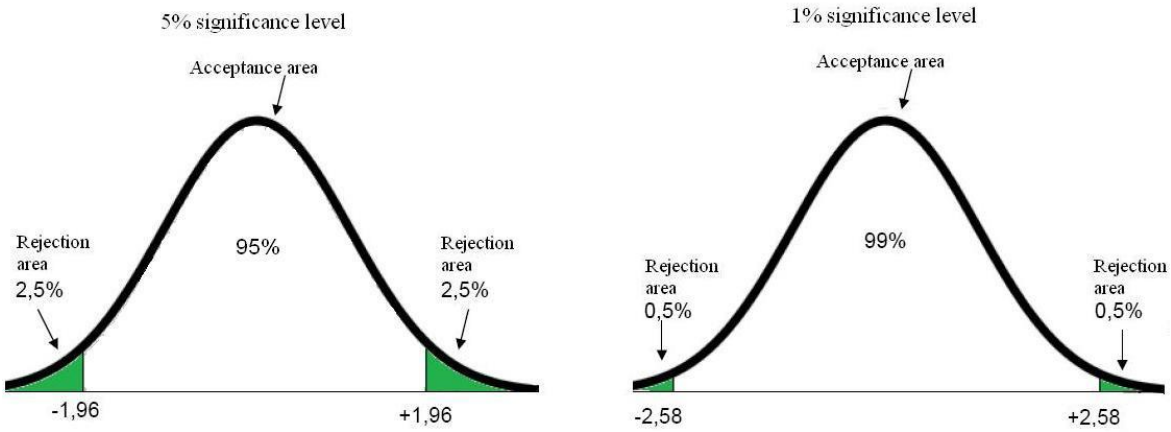

Figure 6. Normal distribution and different significance levels with corresponding cut off values

Also, if auditor is willing to accept 10% probability that deviated frequencies are accidental, then Z-statistics should be set to 1,65.

Although Z-statistics is quite powerful measurement, it may not always be very practical for auditing purpose. Also, it may not be used as an ultimate test of deviation significance in auditing environment. Auditor should not forget statistical environment is quite different from its auditing counterpart. As it is explained in [17, pages 42-43], when any individual value for Z-statistics exceeds 1,96 it may be concluded there is only 5% probability that the difference is caused accidentally. However, this is still quite a big probability and such differences, caused by chance, are quite often in auditing. Also, Z-statistics values are calculated for each digit separately. If we have 9 digits in focus (e.g. in the first digit test), each digit has 5% probability of having accidental Z-statistic greater than 1,96. Then, the chance that at least one of the nine digits will have Z-statistics out of limit is 37%. Furtherly, in performing ten first digit tests it may be expected to find significant Z-statistics proved deviations in close to four cases. Such deviations would typically be completely random, with no practical audit significance. If randomly deviant Z-statistics are relatively common, is this test appropriate at all? How auditor can know which are real deviations and which are just result of random "noise"? Firstly, as it is explained in [17], if the data set simply does not conform to Benford's Law, then typically many columns will have Z-statistics greater than limit level. In such case,

- data may be massively fraudulent,
- data is erroneously extracted,
- data suffers from severe small subset problems, or
- Benford's Law is simply not applicable to data auditor investigates, and data does not conform to Benford's Law

Secondly, which is of most importance to auditor, Z-statistics is only one of approaches to narrow down which digit combination could be fraudulent, erroneous or result of omissions. For example, if auditor investigates tax refund claims and the threshold for non taxable income is 50.000 then a positive deviation of two digit combination "49" is significant because it suggest that the tax payers try to avoid taxation. So, Z-statistics should be accompanied by other investigation methods, particularly by checking the business rules for process execution and data creation.

To furtherly emphasise importance of above statements, we may conclude that for audit purposes it is not enough to use only Z-statistics test in order to confirm whether data are Benford's Law compliant and if data is fraudulent, erroneous or it is resulting from omissions.

6.9.2 Chi-square (χ^2)

Chi-square test is very often used in statistics in order to make conclusion if two data sets, at certain significance level, match each other. In this research it is used for checking if all digits as a whole conform to Benford's Law. It means chi-square test is composite test, like Mean absolute deviation (MAD) test and unlike Z-statistics test.

For each element of data set the chi-square test is calculated as follows:

$$\chi^2 = \frac{(Po - P_{BL})^2}{P_{BL}}$$

where Po stands for the observed (actual) frequency, while P_{BL} is expected Benford's Law frequency. As chi-square is a composite test, it must be calculated for entire observed data set:

$$\chi^2 = \sum_{i=1}^{n} \frac{(Po - P_{BL})^2}{P_{BL}}$$

In order to state Chi-square test proves two data sets are conformed null hypothesis must be accepted as true. A null hypothesis states that observed and Benford's Law distributions are matching each other under certain significance level. Cut-off value for acceptance or rejection of null hypothesis depends on degrees of freedom and significance level. Significance level denotes probability that even if null hypothesis is accepted it is still due to chance alone. In this thesis, significant level will be always set on 5%. Also, the degrees of freedom are calculated as number of observations minus 1. That means the degrees of freedom will be 8, 9, 89 and 899 for the first, the second, the first two digits and the first three digits Benford's Law tests respectively. It means that, according to 8 degrees of freedom and testing on significance level of 5%, in order to confirm null hypothesis that observed and the first digit Benford's Law test distributions are equal, value of χ^2 should be less than 15,507 which is cut-off value.

6.9.3 Mean absolute deviation

Mean absolute deviation (MAD) test may be used as an intuitive goodness of fit measure. Mean absolute deviation is calculated as average of totaled absolute deviations of each data set element.

This measure does not have strictly defined limit values i.e. range in which it can be stated whether deviation of value sets is significant or not. As there are no cut-off values like with Chi-square, there are no strict rules by which auditor can state if certain number set conforms to Benford's Law after applying MAD test. Some examples of MAD use for intuitive explanation if certain number data set conforms to Benford's Law are shown in [19, page 59] and [17, page 79].

For each data set element, absolute deviations (AD) are calculated as follows:

$$AD = \left| \frac{Po}{P_{BL}} - 1 \right| * 100$$

where Po and P_{BL} denote observed and expected frequencies according to Benford's Law.

Mean absolute deviation is calculated for entire data set as follows:

$$MAD = \frac{\sum_{i=1}^{n} ADi}{n}$$

where “n” is total number of elements in data set and “i” is ordinary number of element in set.

Unlike the chi-square and Z-statistics tests, MAD is not affected by the size of observed data set. That means the result is independent on the number of observations itself.

However, in [17] it is stated that MAD is the best conformity test in an auditing context. The author states each auditor has to develop her/his guidelines for measuring conformity using the MAD and those guidelines may vary for different data sets. Certain guidelines are set for MAD cut off levels for disbursement data set [17, pages 118-122]. Based on author’s experience in disbursement audits, MAD cut-off values for the first digit Benford’s Law test are:

- MAD in set [0; 0,4] – close conformity of data set to Benford’s Law
- MAD in set <0,4; 0,8] – acceptable conformity of data set to Benford’s Law
- MAD in set <0,8; 1,2] – marginally acceptable conformity of data set to Benford’s Law
- MAD in set <1,2;∞> - nonconformity of data set to Benford’s Law

However, auditor has to bear in mind that each data set has its own properties and MAD cut-off values. Thus, considerable experience is needed for setting up MAD limits with data set of interest.

7. Design and Verification of Computer Assisted Information Systems Auditing Methodology

As it is indicated in chapter 4, there are different frameworks and approaches for overall business and information systems audit developed by certain authorities. Since auditing activity tends to be extremely complicated and covers different business areas, use of auxiliary auditing methods and tools becomes compulsory. Also, as it is shown in chapter 2, frauds become more and more advanced and resulting in much greater losses. Obviously, existing auditing methods and approaches are not adequate in contemporary business environments.

Although computer assisted auditing is emphasized as important and indispensable by leading organizations in information systems auditing (ISACA), United States banking industry regulation (Federal Reserve Bank), so called „central bank of central banks“ (Bank for International Settlements) and a number of other regulation authorities, widely accepted methodology is still not developed.

In addition, computer assisted auditing methods are used in existing software tools. Methods implemented in computer assisted auditing software are quite extensive in number and modes of use. However, there is no predefined methodology which could more precisely guide auditor while performing audits. As a consequence, each auditor chooses set of methods for each audit activity, use them in different sequences and makes different conclusions. This approach makes computer assisted auditing software not effective enough since audit activities based on such software without use of methodology are arbitrary (depending on auditor's choice), disparate, not standard and non-comparable.

For that reason development of methodology for computer assisted information systems auditing is of the utmost importance. The process for development of such methodology must consist of the following:

1. Definition of specific methods which will constitute the basis of methodology – defining input data, processing algorithm and output data (chapters 5 and 6)
2. Defining general rules and model applicable for any computer assisted information systems auditing methodology resulting in adequate meta-model (chapter 7.1)

3. Defining steps of methodology and appropriate linkage i.e. sequence of methods application depending of output data resulting in adequate model of methodology (chapter 7.2)

7.1 Meta-Model of Computer Assisted Information Systems Auditing Methodology (CAISAM)

Although large number of methods and corresponding computer assisted auditing tools are applied in practice, no specific methodology has been developed. A number of auditors use different methods within different procedures, steps and success. Certainly, such approach has numerous shortcomings resulting in inadequate audit activities, as it is described previously in this paper.

Additionally, in available literature no meta-model of general CAISAM is developed. Such meta-model should be a basis for development of any specific CAISAM. So, first task that should have been accomplished in order to design methodology was development of meta-model of CAISAM.

After general CAISAM meta-model is designed, model of specific CAISAM based on Benford's Law will be created (chapter 7.2). Certain existing methods are chosen and linked into a new and consistent methodology which can be very efficiently used in auditing process and within existing CAATs.

For the purposes of development of specific computer assisted information systems auditing methodology, meta-model is firstly presented (Figure 7) and explained in this paper.

Generally speaking, meta-model is a model of metadata about certain domain. Meta modelling comprises of analysis and construction of models applicable and useful to some domain of problems. A model is a sort of abstraction of specific real world domain, while meta-model is higher level abstraction which emphasizes characteristics of all models form specific real world domain.

Meta model of CAISAM is the abstraction of different possible methodology models covering information systems audit by use of certain data analysis methods. Each such

methodology must consist of processes of data provision, checking of collected audit sample, application of audit methods, checking results of audit method applications, conclusion on eventual fraud, omissions or errors after each audit method is applied and final conclusion on audit process.

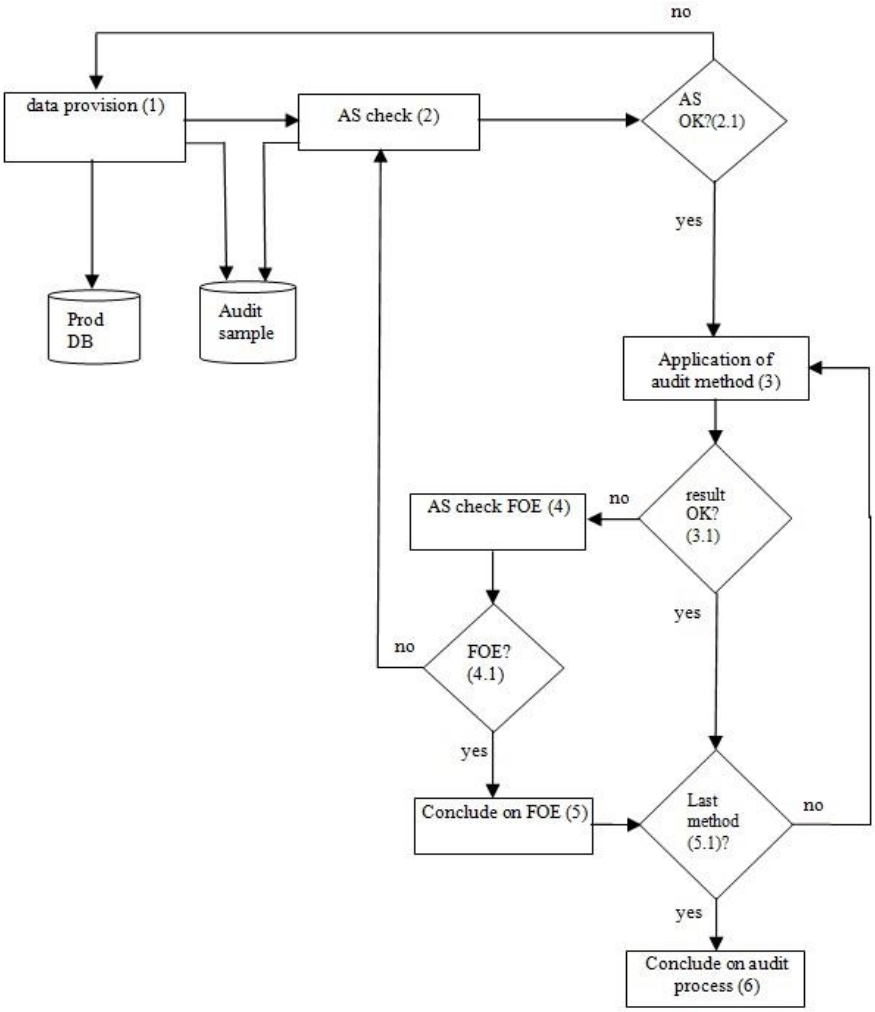

Figure 7. CAISAM Meta-model

The CAISAM meta-model is based on 6 main steps:

1. Data provision
2. Audit sample check
3. Application of audit method
4. Audit sample check on fraud, omission and error
5. Conclusion on fraud, omissions and errors
6. Conclusion on overall audit process

Within each step one or more computer assisted auditing methods are applied. Data provision or data gathering (step 1 on Figure 7) is process of extracting data needed for audit activity from auditee's production database. After data is extracted, it should be stored on hardware and software equipment that is separate from production environment so that audit activity will be executed on non-production infrastructure. There are at least two types of reasons for such approach:

- availability and performance of production database should not be jeopardized by auditing activity
- changes to production data must be prevented.

After audit sample is created, any CAISAM must perform certain steps in order to check relevance and completeness of data (step 2 on Figure 7). Specific methodology must explain which methods should be used and how in this step. If audit sample proved to be adequate (answer "yes" in step 2.1), it may be continued with application of defined auditing method(s) on data (step 3). However, if audit sample was not adequate, data provision process must be reviewed, possibly updated and executed again (step 1). These processes of audit sample checking, reviewing and updating of data provision must be performed until audit sample is proved to be complete and relevant.

After auditor judges that audit sample is adequate, specific computer assisted auditing methods are applied (step 3.). If the output result of specific method is within adequate limits, auditing activity should proceed with next method(s). However, if output resulting from certain method application is out of normal or previously defined boundaries that means auditor must check audit sample on fraud, omission and error (step 4.). This means acquired data must be compared to rules of conduct within specific business entity. If acquired data does not follow business rules and is deviated in fraudulent, erroneous manner or omissions in business conduct are made auditor must conclude on existence of fraud, omissions or errors within business entity (step 5.). It means auditor must explain why and how fraud, error or omission occurred within business entity. However, even in this step it is still possible that data is not deviated because of fraud, omissions or errors but because of inadequate audit sample (“no” in step 4.1) at the first place. If that is the case, audit sample should be re-checked again. It may happen that although audit sample was

checked in step 2., its inadequacy be proved after application of specific auditing method(s) in step 3. As it is shown in model of CAISAM based on Benford's Law explained in chapter 7.2, repeating of audit sample check, review and update should be executed after first audit method (specifically the Benford's Law first digit test in step 3.) has been applied on audit sample. After each method from step 3. in CAISAMs meta-model (Figure 7) is executed ("yes" in step 5.1), auditor must make final conclusions on existence of fraud, omissions or errors i.e. on overall audit process.

In the next chapter, model of specific computer assisted information systems auditing methodology based on the Benford's Law tests is developed. Each step of specific methodology follows meta-model described in this chapter.

7.2 Model of CAISAM Based on Benford's Law

Development of model for a specific CAISAM should be based on meta-model explained previously in chapter 7.1. Specific CAISAM designed in this paper is largely based on Benford's Law (detailed explanation may be found in chapter 6), but also some other methods which are explained in chapter 5 are used.

However, before any actual audit execution, adequate audit planning step should be undertaken. During audit planning phase following prerequisites should be realized:

- clear definition of data structures to be processed including quantity, type, format and layout,
- definition of methods to be undertaken together with ways of methods linkage,
- definition of input and output data,
- determination of resource requirements, i.e. personnel, CAATs, processing environment,
- obtained access to the organisation's information system facilities, programs and data, including database definitions.

As computer assisted auditing techniques software is proved to be extremely efficient in audit examinations, it is necessary to asses usability of such software in certain audit. It must be defined what data in what format will be analyzed. Auditor must in advance define for what time period data should be collected, what the select criteria are, should there be

any aggregate functions applied, what registries are indispensable, are there any joins with other data tables that should be involved. Concerning the way of accessing data, it must be settled if data will be accessed off-line or on-line. If access method is off-line, which is the most usual, it is to be decided about export format. The most usual export formats are ASCII delimited and ASCII fixed width files. In both cases auditor must require certain file structure which encloses sequence of columns, data type of each column, eventual heading record and eventually final record in data file. As a rule, on-line access method should be avoided because of possible performance degradation and risk of unauthorized changes. If it is indispensable to access data in on-line mode, it should be done out of business hours or at least when information system database is used minimally and without update, delete or insert data access privileges. Also, it must be agreed what technical prerequisites are needed for establishing database connection (e.g. installation of database drivers). As it is already briefly indicated, one more obstacle which should be carefully discussed and agreed upon is definition of user and his access privileges in target database. User must be named and with read only (select) privileges. Additionally, all activities on database during on-line access must be monitored and logged in audit trails. Technical requirements must be agreed by IT department, while requirements concerning scope of data (content) must be demanded by the department who is the owner of the data.

After planning steps for computer assisted auditing are completed, execution of specific auditing activity should commence.

Crucial prerequisite for computer audit commencement is understanding of data, data structures and appropriate mapping or relating data to business processes and events. Developed computer assisted information systems auditing methodology covers methods and steps that must be undertaken in the audit execution phase of audit process. Audit planning, documentation and reporting should be done in accordance with description in chapters 8.1.1, 8.1.3 and 8.1.4.

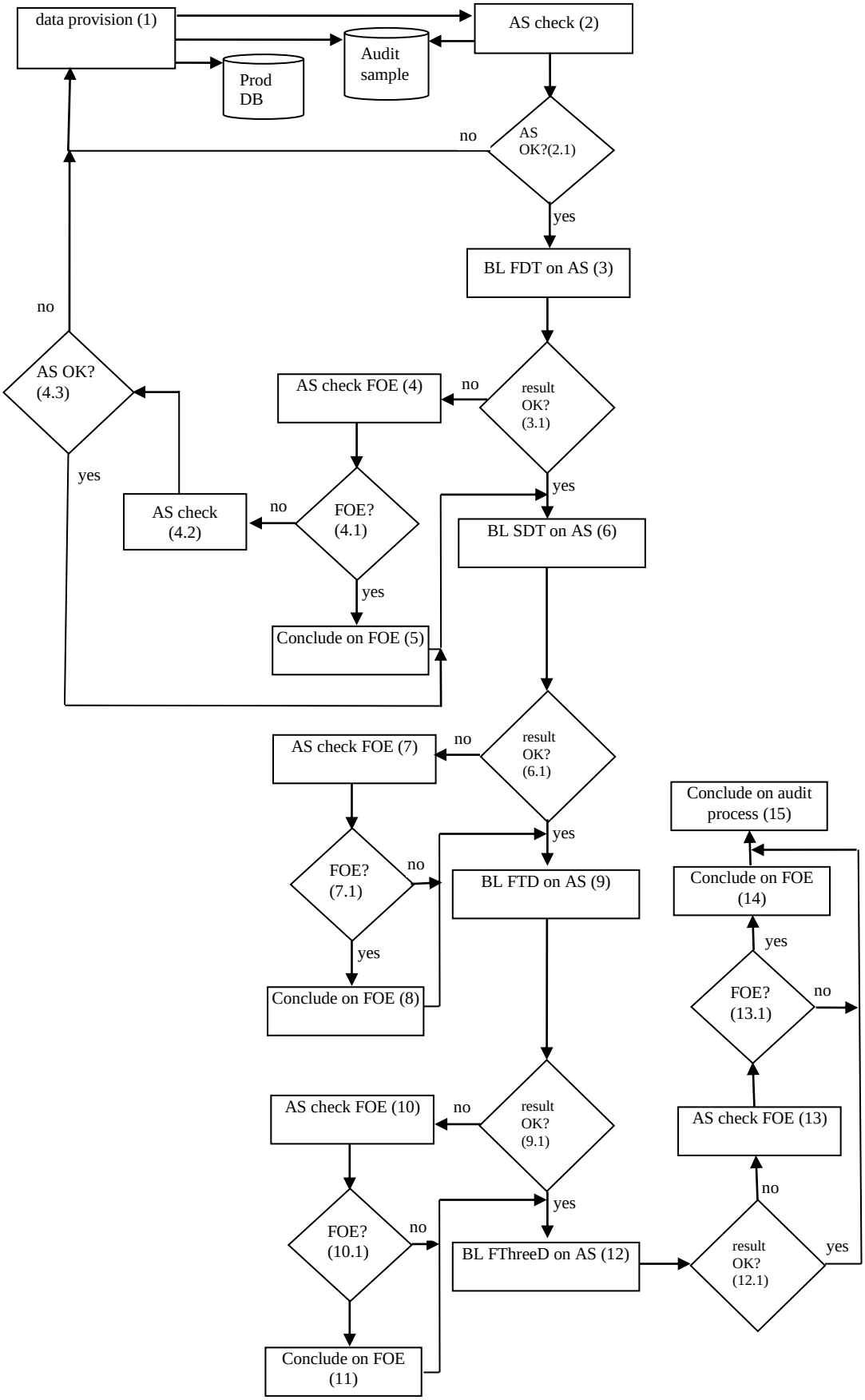

Figure 8. CAISAM Model

First step (step 1 in Figure 8) in developed computer assisted information systems auditing methodology is data provision. During this step auditor must define ways of taking over data from production databases. It is indispensable that statements for data provision are clearly defined and that conditions are appropriately constructed. As already mentioned, one of major cares in computer assisted auditing is the quality of provisioned data. If data is not appropriately provisioned, the whole auditing process will most certainly fail. The objective of the first step is to ensure that data are ready for auditing i.e. relevant and comprehensive. This step includes usage of following methods:

- selection – in order to declare which data are relevant for audit, to obtain comprehensiveness or completeness of data
- join – in order to combine data from different data tables (relations) or even from different data sources

Typical examples for this step is definition of SQL conditions according to period, types of transactions, certain departments, supplier, customer etc. Auditor should bear in mind that created selections and joins must be compatible with production database systems on which they will be applied. Although almost all modern databases are based on SQL standards, still there are slight differences.

Then abovementioned methods must be applied to production database.

After audit sample (AS) is created out of production database, auditor must check its relevance and completeness (step 2). This step must be executed because of following reasons:

1. It is possible that auditor's knowledge of data and data structures was not sufficient so planning phase and step 1 outcome in inadequate conclusions. Final results are SQL statements which produced incomplete or non relevant data. During this step auditor may correct wrong assumptions and improve his knowledge about data and data structures.
2. In some cases IT personnel will execute SQL queries prepared by the auditor. Since auditor will not be able to monitor process of database log on and queries execution, there is possibility queries may have been changed and/or data have been accessed from non production database (development, testing, data warehousing, temporary).

Of course, if planning phase of computer assisted auditing process was performed correctly and in step 1 data was provisioned according to created queries, then step 2 will confirm relevance and completeness.

Methods that should be used for data relevance and completeness check are selection, summarization (grouping), stratification and join.

For example, selection may be used in order to check if some specific data type (e.g. transaction type) is extracted in certain time period. Summarization may confirm if all data types (e.g. all transaction types) are excluded from production database. This method will clearly show if some data type does not exist in audit sample. Stratification may be set as first required method in data relevance and completeness check. After initial strata are created, auditor may be able to notice discrepancy between expected and actual data set. Stratification will produce strata according to auditor's instructions (e.g. transaction amount) which may show some data subsets were omitted from production database. This may be noticed if some strata lack data i.e. if there are problems with data segments. If that is a case, auditor may question created audit sample. Of course, it is useful to additionally check deviated strata. Join method should be used whenever relevance and completeness check is dependent on relations between audit sample and data in other tables or databases. Except natural or equi-join, auditor should concentrate on left and right outer joins. With outer joins it is possible to check if some data types in audit sample are missing.

Additional selection and summarization together with auditors experience and expectations may be used in questioning data with data and business process owner. Also, following additional checks may be performed:

- comparison of data in audit sample with data subsets from previous audits
- comparison of data in audit sample with data from other databases storing same or similarly organized data (e.g. data warehousing, data backups)
- comparison of data in audit sample with data in some other formats (e.g. paper) and/or with data from other sources (e.g. facility management system, vacation data, accounting data, data, application and event logs, data from corresponding business entities – e.g. suppliers, tax authorities, customers).

If auditor has reason to discard audit sample as incomplete and non relevant, step 1 has to be repeated. Of course, auditor should mitigate reasons that resulted in inappropriate audit sample in the first place.

Following actions should be taken in order to get relevant and complete audit sample:
- auditor has to review his knowledge of data, data structure and business being audited
- auditor must work closer with IT personnel in preparation and execution of SQL statements

Another problem that may appear is that audit sample contains excessive data which means data was collected on much broader scope than required by auditor. For example, auditor may have required only selected types of payments in order to increase the focus on data but resulting audit sample contains all payment types. That way, focus may be lost and investigation of errors, omissions and fraud more complicated. Benford's Law method, on which CAISAM is based, requires more focused audit samples. If audit sample is too general, even if there are obvious deviations from Benford's Law, it may become quite cumbersome to relate deviations to business reasons. So, search for errors, omissions and frauds could take much more time than planned. A remedy for situation when audit sample has more data than necessary can be:

- Audit sample is generated again from the original data. That means auditor must require more specific data, thus define data conditions that IT personnel will again execute on production database.
- Audit sample set will be narrowed down from original audit sample. That means auditor must extract needed data, discard unwanted data, and create new, more focused audit sample. The extraction is done by use of selection method and application of appropriate extraction condition. Surely, this option is more practical and will be used in most of the cases. It also has additional advantage of improving auditor's knowledge of data even before the methods for investigation of omissions, errors or frauds were applied on data.

Steps 1 and 2 have to be repeated until auditor accepts data set as relevant and complete. When and if chosen data set is accepted as relevant and complete, next method that should be executed is test of first digit Benford’s Law (step 3). The first digit Benford’s Law test will result in 9 data subsets (digits 1-9). Quite often, the first digit Benford’s Law test will

not be focused enough and will not give enough proof whether data is fraudulent, erroneous and/or not complete. Even if data subsets will significantly deviate from Benford's Law distribution, usually auditor will not be able to make conclusions why deviations occurred.

Data distributions should be compared to the Benford's Law first test distributions in order to check for conformity. Conformity should be examined by chi-square test, mean absolute deviation test or Z-statistics test. How conformity tests should be applied is explained in chapter 6.9 and in [11]. Diagrams should be used in order to perform visual inspection of data distributions and their deviations. If data does not follow predefined distributions ("no" result in step 3.1), auditor must check if data is fraudulent, erroneous and/or data resulted from omissions. This check must be performed in step 4.

However, if data satisfies Benford's Law first digit distributions ("yes" result in step 3.1), next Benford's Law test should be applied on data (step 6).

Concerning step 4 (audit sample check on fraud, omissions and errors – "AS check FOE") and 4.1 (conclusion on existence of fraud, omissions and errors – "FOE?") auditor has to understand rules of business conduct especially in relation to limits (e.g. according to authorization for payments, tax obligations and bonus gains), regularly recurring events for certain calculations (e.g. existence of regular interest calculation), rules for calculated database fields (e.g. tax calculations), etc. Limit avoidances resulting in pushing certain amounts bellow or over predefined limits are rather often, so auditor should be aware of their existence. After Benford's Law test shows deviations, additional checks on data should be based on selection, summarization, duplication and rounded values checking methods. Auditor must understand if there are specific reasons why data does not follow Benford's Law. If numbers are clustered around certain limits and clustering can be related to limits set by management than there is high probability of committed fraud. It is important to notice steps 4 and 4.1 have to be repeated after each Benford's Law tests resulting in deviations (steps 7, 7.1, 10, 10.1, 13, 13.1).

If tests against Benford's Law significantly deviate, auditor may perform some additional tests only for certain digits which deviate from Benford's Law frequencies in order to check against fraudulent or erroneous activity. Examples of use of certain analysis tests in steps 4, 7, 10 and 13 after each Benford's Law test shown discrepancies are:

- finding rounded amounts, amounts starting with multiplies of 10 or 100 (rounded values method)
- counting frequency for each amount – searching for multiple occurrences (number duplication) of the same amounts especially in short period of time (duplication method)
- finding rounded and duplicated amounts on very same day (rounded values, duplication and summarization methods)
- searching for rounded and duplicated crediting amounts for certain accounts in specific period of time (rounded values, duplication and summarization methods)
- rounded and duplicated crediting amounts by detecting specific employees (rounded amounts, duplication and join methods)
- amounts slightly below certain threshold – this checks if payer or payee wanted to evade entering certain tax limits or additional checks by authorities (selection method)
- finding amounts slightly greater than certain threshold – sometimes business entities with performance (sales, investments, contracted amounts etc.) above certain limits may get special status in their relationships with state authorities, banks or other business entities (selection method)
- multiple payments of same type paid same day (or in short time interval) with sum above or below certain threshold (summarization, selection and join methods)

On the contrary, if auditor can not relate clustering, i.e. non conformance to Benford's Law distributions, to evasion of certain business rules, it is possible data set simply does not follow Benford's Law first digit distribution. Auditor may conclude deviations from first digit Benford's Law distributions are result of normal business conduct. As it is already stated, more focused tests should be applied on data. Use of selection, summarization, number duplication and rounded values checks are required. Using these methods auditor can focus on data causing deviations, after selecting and summarizing according to defined criteria. One reasonable example is selection of certain types of transactions committed by certain employees. Then number duplication and rounded values check may be applied on some number subsets. If considerable number of values falling into come clusters is duplicated or rounded, perhaps fraudulent behaviour is on scene.

Also, if application of selection method showed clustering of transactions in certain time period, then summarization of transactions according to certain employee and transaction type in relevant period could be of special audit focus. Additional review based on duplication and rounded values should be also performed.

Nevertheless, even if it is possible to make conclusions about fraud, omissions and/or errors solely on the first digit Benford's Law test, it is indispensable to continue with next Benford's Law test. It is the second digit Benford's Law test (step 6). This is mandatory, since other types of deviations may be spotted after application of rest of Benford's Law tests.

However, if data are deviated from the Benford's Law first digit test and there is no proof of fraud, omissions or errors in business conduct, auditor must again check audit sample data on relevance and completeness (step 4.2). It is possible that first check on relevance and completeness performed in step 2 was not adequate and that auditor made wrong conclusions. In auditing work it is possible to commit such wrong judgement which is the most often consequence of:

- insufficient knowledge of business system and underlying data (resulting in wrongly performed step 1)
- inadequate application of selection, summarization, join and/or stratification methods (step 2)
- insufficient knowledge of underlying data organization and structure (steps 1 and 2)

If auditor believes there is considerable possibility that data is not fraudulent but not relevant and complete ("no" result in step 4.3), data provision must be repeated. The same methods as in step 1 and 2 may be carried out after auditor additionally improves his knowledge of business system, data organization and data structure. Of course, extensive knowledge on methods in focus is indispensable. So, steps 1 and 2 must be accomplished again not bearing in mind that data was not appropriately sampled and checked in first place. Also, there is possibility that data is relevant and complete but simply not enough focused. If audit sample is not focused enough, but consist of data from different business entities, various types of transactions within business entity or whole industry branch (as it will be shown in chapter 7.3.3) then CAISAM will not be efficient. It is a normal consequence since the gaining of focus is prerequisite for adequate audit of business

function or process. So, capability to clearly relate data to auditable business process or business entity is indispensable condition for effective CAISAM.

If, after additional checks, it is concluded data is relevant and complete ("yes" result in step 4.3), auditor should proceed with Benford's Law testing. The second digit test (step 6 – "BL SDT on AS") should be next in sequence. This test is also fairly broad, not very focused on certain data subject and usually will not be enough for final judgement on eventual fraudulent, omitted and/or erroneous data. The second digit test will show distribution of second digits in observed amounts and similar to the first digit test it is not very efficient auditing method. It results in only 10 data subsets (digits 0 to 9). Such small number of resulting subsets has consequence of quite large proportions. Any of 10 subsets will often be too large for audit conclusions. However, the second digit test may show significant deviations which may be reflection of certain limits evasions resulting in number clustering.

Comparing to steps that follow after first digit Benford's Law, there is slight difference in steps following the second digit test. Namely, auditor does not have to recheck on relevance and completeness of audit sample. So, there is no "AS OK?" check which was mandatory if fraud, omissions and/or errors check were not found after noticed discrepancies in the first digit tests. This is the result of experience - it may be said if audit sample was checked twice (steps 2 and 4.2) that auditor finally extracted appropriate i.e. complete and relevant data from database.

The rest of steps following immediately after the Benford's Law second digit test (steps 6.1, 7, 7.1, and 8) are in essence coherent with corresponding steps performed after Benford's Law first digit test (steps 3.1, 4, 4.1 and 5).

However, it is possible that step 1 resulted in reasonably focused data set i.e. audit sample. If it is so, there is higher probability that already the first and/or the second digit Benford's Law test and following selections, summarizations, duplication and rounded values checking methods will be enough for conclusions on some fraud, omissions and/or errors in business system. Although in some cases deviations of data set from Benford's Law first and second digit distribution are easily explained after additional focusing by selection, summarization, duplication and rounded values checking methods auditor has to continue with more focused Benford's Law tests, specifically the first two digits and the first three

digits tests. These tests could give additional information and conclusion why deviations occurred. Also, if no deviations where noticed by the first and the second digit tests it is mandatory to accomplish the first two and the first three digit Benford's Law tests. As it is already stated, these tests are much more focused and their application result in much focused audit samples so the conclusions about certain deviations may be more precise.

The first two digits Benford's Law test (step 9) has much more audit relevance than the first digit and the second digit tests. It is more focused since it takes into account 90 combinations of first two left most digits. The first two digits test is much more sensible (in theory exactly 9 times) than the first digit test. This means auditor will have much more potential in noticing deviations and recovering fraud, omissions and/or mistakes in business activity. After performing this test, auditor can spot finer irregularities or discrepancies and then perform additional analysis with other methods (summarization, selection, rounded amount, duplication, join) belonging to CAISAM methodology as shown in step 4. Each significant deviation on the first two digits should be thoroughly checked and compared to certain business rules (steps 10 and 10.1). Furtherly, whatever is outcome of step 10.1 (deviations are result of fraud, omissions and/or errors or not), next and final Benford's Law test must be executed on audit sample.

The first three digits test (step 12) is the most specific of all Benford's Law tests. It is highly focused because it gives considerably smaller subsets than any other Benford's Law test. This test covers 900 three leftmost combinations (digits 100 to 999 inclusive). It is 9 times more sensible than the first two digits test. Since it has greater precision it will be the best choice for recovering abnormal data duplications. So, duplication method should be performed with more care especially for three digits combinations that are deviated from Benford's Law distribution. Also, this test will be much more beneficial for analysis and conclusions on clusters or so called "positive spikes" on diagram representations resulted from deviations from Benford's Law distribution. Background for explanation why this test is more efficient in cluster analysis is the same as for duplications: test is simply more focused, resulting in larger number of subsets (900) what causes smaller average number of elements in audit subsets. Apart from that, steps 12.1 to 14 are already appropriately described in previous paragraph on the Benford's Law first two digits test.

After conclusion on existence of fraud, omissions and errors concerning the first three digits test (step 14), auditor has to review whole audit process defined by methodology and

make final conclusions. This step is necessary as individual tests may show different deviations so auditor may discover various discrepancies resulted from fraud, errors and/or omissions.

7.3 Verification of Designed Methodology

The designed methodology will be verified in practical audit activity. For the purpose of verification, methodology will be used in auditing of cross-border payments system data. These data are collected by Croatian National Bank which uses them for purposes of balances of payments of Republic of Croatia, as well as for auditing and control purposes.

7.3.1 Description of Cross-border Payments System

Cross-border payments system includes all payments on the basis of import and export of goods, services and other payments between domestic and foreign entities (individual or business). In the Republic of Croatia, cross-border payments are transacted by banks which have approval of Croatian National Bank.

Basically, there are two categories of transaction payments in cross-border payments system:

- domestically initiated payments for imported goods or abroad services (ordering payments)
- collection payments received from abroad for exported goods or services (receiving payments)

Each transaction must be documented in specific type of payment document within bank receiving or ordering payment. All payment transactions must be collected and sent to Croatian National Bank on monthly basis in strictly defined file format. Banks must follow formal and logical instructions which define how each payment transaction should be recorded within data file. If Croatian National Bank finds any formal or logical errors in data file, it informs bank about it, demands fixing and resending of data.

The most important attributes in payment transactions are the following: bank code, account number, code of payment purpose, type of payment document, date of transaction,

currency, amount, country of order/receiving payment, code of payer (if it is payment order).

When receiving payment transactions data file, Croatian National Bank calculates some additional attributes (columns). The most important are amount in kunas, amount in US dollars and amount in euros.

One of the attributes in considerable focus of analysts is code of payment purpose. That attribute holds information which is necessary for determination of reason of payment i.e. why and for what payment was received or ordered. Some of payment purposes are:

- goods – goods that can be transported and which change the ownership between domestic and foreign business entities or individuals.
- military weapons and other military equipment
- cargo maritime transport
- passenger maritime transport
- cargo air transport
- passenger air transport
- railway cargo transport
- railway passenger transport
- road cargo transport
- road passenger transport
- river cargo transport
- river passenger transport
- pipeline transport of oil and gas
- tourist traveller charges
- charges for scholarships and education
- business trips
- telecommunication services
- construction works abroad done by domestic companies
- construction works in Croatia done by foreign companies
- insurance premiums
- insurance claims
- financial services fees
- consulting services

- fees and salaries of employees – abroad and inland
- stock dividends
- shares from profit
- interests earned and paid
- money transfers – workers transfers
- pensions, disabled support fees and social expenditures
- financial transactions – purchasing stocks
- loans – short term
- loans – long term
- money deposits
- options
- currency exchange
- transfers of foreign currency between domestic banks

Combination of code of payment purpose and type of payment document is sufficient for realizing if certain payment is received from abroad or ordered to abroad. Considering very detailed and excessive information about each payment is reported to Croatian National Bank, it is possible to control and audit how cross-border payments are initiated and transacted.

Also, Croatian National Bank regularly uses collected data in order to create and control the balance of payments of Republic of Croatia. So, income and expenditures can be very effectively monitored with the aim to react if necessary.

7.3.2 Requirements on Cross-border Payments System Auditing

Objective is set to perform data audit of cross-border payments i.e. cross-border payment messages ordered or received by Croatian commercial banks and central bank. Since these data are confidential, no information on any single payment message, any single bank or any single payer will be presented. Data that are included into in this examination are from period 1st of February to 30th of April 2008 which totalled in 1.745.311 payment messages.

Doubtlessly, exchange of various goods between Croatia and foreign economies is in constant focus of Croatian economists. Lot of economy analytics consider that information on this exchange shows status of Croatian economy. Changes in economy are often

described and explained by changes in foreign exchange and values exported or imported. Not bearing in mind considerable dependency of national and world economies on these parameters, it is especially interesting to answer the question if it is possible to note whether there are some irregularities or deviations in creation of payment messages i.e. payment amounts. Amounts in original currency should be analyzed for certain groups of transactions (e.g. received payments for exported goods) as well as for all payment transactions. Special treatment should be given to data subsets that are deviated from Benford's Law distributions.

Checking on possible fraud, omission and error should be performed on entire collected data set. Data should be audited by computer assisted information systems auditing methodology (CAISAM) developed in chapter 7.2. After data is provisioned and audit set is checked on completeness and reasonableness examination should commence by use of Benford's Law. Examination of conformity with Benford's law according to first, second, first two and first three digits i.e. examination of frequencies of certain first, second, first two and first three digits in payment amounts must be included, as described in CAISAM.

During the audit, additional care should be given to analysis of payment purposes. Whenever some deviation occurs according to Benford's Law analysis, summarization or selection according to certain payments purposes should be performed. The reason why payment purpose should be in the audit focus is because of very important information on nature and intention of payment that it contains. Afterwards, very useful information may be gained from selection and summarization according to certain amounts which show excessive appearance according to Benford's Law distribution within payment purpose in focus. For example, if it is observed that first digit "2" is non-conformant to Benford's Law, first action could be summarization with payment purpose as aggregation base attribute, and count as aggregation function. That way, auditor may note which payment purposes are deviated i.e. which payment purposes mostly take part in the deviation. Also, auditor may choose amount (or amount in euro/dollar) as aggregation values attribute on which sum or average calculation is performed. After summarization, only the largest data subsets of certain payment purposes should be furtherly investigated. The very effective yet reasonably simple methods are rounded values and duplication check. Auditor should recover the most repeated values in data subset of certain payment purpose. If those amounts which are the most often are not rounded, than additional search for rounded

values should be done. That way auditor can find out if number invention occurred while bearing in mind that number invention is very often consequence of fraud, omission or error. Of course, summarization and selections on banks and some other attributes can be advisable.

Since cross-border payment system generates huge volumes of data, appropriate increase of data focus is of a crucial importance. Increase of data focus is achieved by choosing certain data subsets. It can be done by selection, summarization or even stratification. After those methods are applied, search for rounded and duplicated values may follow. Auditor should understand data patterns of cross-border payments in order to adequately explain clustering of values and deviations from Benford's Law.

7.3.3 Cross-border Payments System Auditing

The principal objective of this chapter is to perform auditing of cross-border payment system in accordance with computer assisted information systems auditing methodology designed in chapter 7.2. So, auditing process is focused on data created in cross-border payments i.e. payment messages.

Audit process included payment messages in Croatian banking system in period between 1st of February 2008 and 30th of April 2008. The following are the most interesting data that were in focus of audit process:

- date of transaction
- amount (in original currency)
- amount in kunas
- amount in EUR
- code of payment purpose
- bank code
- type of payment document

Total number of data rows of cross-border payment messages in observed period was 1.745.311.

Chi-square (χ^2), Z-statistics and Mean Absolute Deviation (MAD) tests are used in order to evaluate conformance of payment amounts with Benford's Law. The objective was to show

if eventual deviations of frequencies of observed phenomena from Benford's Law frequencies are incidental or not i.e. if frequencies follow Benford's Law. A goal was also to compare practical usefulness and note differences between these conformity tests in auditing environment.

According to computer assisted information systems auditing methodology, first step of audit process that follows after strictly established audit plan is data provision. Data provision process should ensure that data are adequately extracted from production database. That means extracted data is relevant and complete.

For the purpose of audit, records on cross-border payments were extracted with only one restriction: date of transaction. Only transaction committed between 1st of February and 30th of April 2008 were included in the audit process. Data provision statement was based on selection method and was very simple:

```
SELECT date_of_transaction, amount in original_currency, amount_in_HRK,
amount_in_EUR, code_of_payment_purpose, bank_code
FROM cross_border_payments
WHERE date_of_transaction BETWEEN "01-FEB-08" AND "30-APR-08";
```

Above statement was prepared in Oracle syntax since data on cross-border payments is stored in Oracle database management system. However, statement is written in accordance to SQL standard, so it can be applied in any contemporary database management system with only minor changes.

Data table containing cross-border payment transactions also has two related data tables which provide important three columns for each individual transaction (bank_code, code of payment purpose and type of payment document). Without these columns, it would not be possible to determine which bank issued the payment, what the type of the payment was and what original payment document was used for payment initiation. These columns contain only codes of three described attributes, not descriptions. Descriptions are stored in separate three tables. This work is not focused on any specific bank, but will audit different types of payment messages for the whole banking industry. Also, Croatian National Bank which provided cross-border payment messages gave permission for examination of data, but without disclosing any information about any specific bank and any individual

payment transaction record. So bank codes and related banks were not in a focus of audit process.

Code of payment purpose contains description in form of a fixed list stored in related data table. However, since list is static and constrained concerning a number of records it was not necessary to perform join of tables with cross-border payment transactions and payment purposes. The same is worth for table containing description of types of payment documents.

Even if joins of bank table, payment purposes table and payment documents table with cross-border transaction were performed that would only give additional description of records. However, in this case, additional description would not assure any crucial information for significant improvement of audit activity quality.

Delimited ASCII text file was required export format. So, no direct access on production database was performed by computer assisted auditing tool software. Procedures of database logon, execution of select statement, export of selected records to a text file and copying of created text file to auditor's computer environment was performed by IT database administrator. Those steps have been under constant supervision of auditor, in order to assure complete and relevant audit sample. Prerequisites for efficient supervision are knowledge of auditor in specific IT infrastructure configuration (database and operating systems) as well as data structure in specific database.

According to step 2 of CAISAM, audit sample has to be checked on data relevance and completeness. As noted in chapter 7.2, methods that can be used for audit sample check are stratification, join, summarization and selection. The first test performed on data sample was based on stratification method. Data was stratified on transaction date, with 7 days periods starting on Fridays and ending on Thursdays. The only exception was the last week ending on Wednesday (30th of April 2008) because that was the last day on which transactions were extracted.

stratum no	date from (inc)	date to(ex)	no of records	% of records
1	1.2.2008	8.2.2008	121.419	6,96
2	8.2.2008	15.2.2008	125.859	7,21
3	15.2.2008	22.2.2008	128.186	7,34

4	22.2.2008	29.2.2008	129.961	7,45
5	29.2.2008	7.3.2008	134.504	7,71
6	7.3.2008	14.3.2008	138.123	7,91
7	14.3.2008	21.3.2008	142.769	8,18
8	21.3.2008	28.3.2008	84.607	4,85
9	28.3.2008	4.4.2008	157.837	9,04
10	4.4.2008	11.4.2008	145.462	8,33
11	11.4.2008	18.4.2008	150.499	8,62
12	18.4.2008	25.4.2008	154.793	8,87
13	25.4.2008	2.5.2008	131.292	7,52
			1.745.311	
		LLE	0	0
		ULE	0	0

Table 13. Stratification according to 7 days strata periods applied on transaction dates

Column “date from (inc)” contains beginning date of strata. That dates are included when calculating membership in each strata. Column “date to (ex)” contains ending date of strata for which transactions are not included when calculating strata. Each stratum has one weekend, starting and ending on each day of the week, which should have eliminate consequences of different weekdays in some strata. It can easily be noticed number of transactions (“no of records”) slowly grows with almost every next with exceptions of 8th, 9th and 13th week. The growth of number of transactions in each consecutive week from February to April is normal seasonal behaviour. At the beginning of year (January) the number of transactions is usually the smallest and rising until May inclusively. Drop in number of transactions in 8th week can be justified by Easter Sunday which fell on 23rd of March and Easter Monday which fell on 24th of March. Even on Saturday, 22nd of March, number of transactions was lower than on usual Saturday. A significant rise in number of transactions in 9th week can also be explained by Easter. After the Easter, lot of transactions postponed from week following the Easter were committed in 9th week. Lack of records in last week can be justified with a fact that it had only five working days since 1st of May was not included in the audit sample and is also a national holiday in Republic of Croatia. Also, it is shown that according to transaction date there were no upper (ULE) or lower (LLE) level exceptions.

Furthermore, summarization and join methods were applied in order to check audit sample. This time, different column in data table was used in order to check relevance and completeness of audit sample. Summarization column was code of payment purpose. The objective was to check if all relevant codes of payment purpose were selected into audit sample i.e. if some were omitted. Summarization shown there were 93 different payment purposes in audit sample. After the completion of summarization, outer join with payment purposes table was executed. The common column used as a basis of outer join was code of payment purpose. The objective was to check if some payment purposes are not found in extracted audit sample but otherwise exist in list of payment purposes table. However, all usual payment purposes were found in audit sample. The most representative were banking deposits, payments for goods, financial services, buying and selling of currency in exchange transactions and traveller payments. Summarization and outer join results were in accordance with expectations.

After these steps, it could have been confirmed that audit sample was relevant and complete.

After audit sample check, the first digit Benford's Law test was applied on data (step 3 of CAISAM). Analysis was based on payment amounts in original currency. The results are shown in Table 14.

D	fo	fs	fs-fo	Po	χ^2	Z
1	525.392	565.119	39.727	7,56	3.003,94	65,56
2	307.335	318.481	11.146	3,63	404,26	22,16
3	218.057	211.775	-6.282	-2,88	181,00	14,39
4	169.138	151.429	-17.709	-10,47	1.854,24	45,31
5	138.196	163.018	24.822	17,96	4.458,34	69,59
6	116.843	102.665	-14.178	-12,13	1.720,43	42,96
7	101.214	92.205	-9.009	-8,90	801,91	29,17
8	89.277	73.562	-15.715	-17,60	2.766,30	53,98
9	79.861	67.057	-12.804	-16,03	2.052,90	46,40
	Total:	1.745.311		10,80	17.243,32	

Table 14. First digit (d) analysis of amounts in original currency for all payments

Explanation of used symbols:
fo – expected frequency – number of observations expected according to Benford's Law
fs – actual frequency
fs-fo – difference between actual and expected frequency
Po – percentage of deviation of actual from expected frequency
MAD – Mean Absolute Deviation - average deviation from percentages of deviation (sum of absolute values Po divided by number of frequency categories i.e. 9)
Z – Z-statistics for fs values with respect to fo values

In order to perform Chi-square test, a null hypothesis was set and significance level tested on 5%. According to 8 degrees of freedom and testing on significance level of 5%, in order to confirm our first hypothesis, value of χ^2 should be less than 15,507. Since it is not the case, assumption that number set of cross-border payment amounts in original currencies conform to Benford's Law according to chi-square test should be reject. It can easily be noted that significant (positive) deviations exist for digits 1 and 5 i. e. there is notable surplus of payment amounts in original currency with digits 1 and 5.

For Z-statistics 5% significance level is set which means there is only 5% probability that difference between actual and expected frequency values is accidental. Cut off value for each Z-statistics value is 1,96. All values that exceed this value should be flagged as they deviate according to Z-statistics. In our case it is easily observed that all individual frequencies are far exceeding the Z-statistics cut off value. As with chi-square analysis, it can be concluded that the largest deviations are for digits 1 and 5.

MAD consists of three components. Deviation (Po) measures difference between actual and expected frequency. In Table 14 it can be noticed that for first digit 1 the actual frequency (fo) is 525.392, expected frequency is 565.119. Deviation may be denoted in percentage values as it is shown in Table 14. Second component is absolute function which is applied to all deviations. Third component is the mean which is total of absolute deviations divided by number of frequency categories (9). The largest individual positive deviation according to MAD is for digit 5, which is in surplus for almost 18% when compared with Benford’s Law expected frequency. Digits 1 (+7,56%) and 2 (3,63%) are also in surplus. As a contrast, all other digits are in deficiency. Usually in the auditing context digits that are in surplus according to conformance tests deserve additional

attention. Auditors should carefully and furtherly investigate what is in a background of surpluses. Digits in deficiency usually do not deserve audit focus and too much additional work because their shortage is only the reflection of before mentioned surpluses.

It is clear from first digit analysis that banks are paying and receiving payment in amounts with first digits 1 and 5 more often than expected according to Benford's Law.

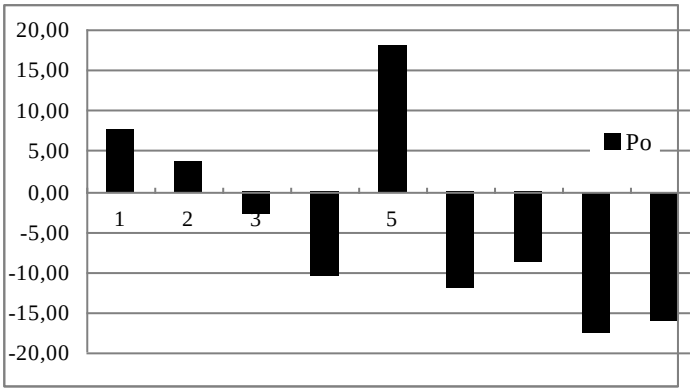

Figure 9. Frequency deviation from Benford's Law for first digit for all payments in original currency

However, since data obviously do not follow first digit Benford's Law (step 3.1), audit sample should be furtherly analysed in order to eventually find frauds, errors or omissions.

It is not correct to immediately state that irregularities exist because of fraudulent behaviour or errors. The first digit Benford's Law test is not focused enough so it is usually good only as a starting point of data analysis. For correct conclusion concerning this phenomenon additional data from business entities (companies, state organizations and agencies) and individuals should be investigated as well as other Benford's Law tests must be applied. According to deviations spotted after the first digit test, it may be assumed business entities and individuals pay their invoices and get paid in amounts which are significantly more often results of rounding and psychology of payer than exact calculations. Since audit sample is too large, consisting of all transactions of all types for all banks during three months period it may be stated that although within steps 2 and 2.1 of CAISAM it was concluded audit sample is relevant and complete, it is not focused enough. For purposes of audit, it would be necessary to narrow down audit sample. That means, some data in audit sample should be additionally extracted in order to focus on

business activity that can be concretely analysed and compared with specific business activity.

Also in the step 4, auditor should focus on data which caused deviation and perform additional analysis. Analysis may be based on selection, summarization, rounded values and duplication methods. In this case, it means further inspection should be performed on payment messages which payment amounts start with digits "1" and "5". Analysis may be provided by summarization method where aggregation base attribute (column) was code of payment purpose and summarization function was count of records. This application of summarization method resulted in generation of groups according to each unique payment purpose. For each group, number of actual transactions was counted. It was realized that only two payment types had significant deviations – all other payment types were in accordance with Benford's Law. The following payment types have significant surplus of transactions having starting digit "1" in payment amount:

- banking deposits (code of payment 870) - in total 96.684 records which is more than 17% of all records starting with digit "1"
- buying and selling of currency (currency exchange transactions, code of payment 912) - in total 32.056 transactions which is 6% of all transactions starting with digit "1"

If these two payment types did not have such significant surpluses, the Benford's Law first digit test would not indicate excess of 39.727 records (deviation of 7,56% from expected frequency) starting with digit "1" (Table 14). So, these payment types deserve additional attention and explanation.

Banking deposits are payments resulting from acceptance and withdrawal of capital denominated in foreign currency. It is known that clustering of numbers is usual with individual payments related to deposits. Further investigation shown that considerable rounding and duplication appeared in this particular case (Table 15):

amount	no of records
100	4.936
150	1.129
1.000,00	5.386
1.500,00	1.975

10.000,00	1.860
10.500,00	443
total:	15.729

Table 15. Specific rounded and duplicated payments amounts (deposits)

Data in Table 15 shows that 5.386 payment messages with amount 10.000 in original currency resulted in deposit or withdrawal from the bank i.e. related to deposit type of payment. Total of 15.729 rounded and duplicated payment amounts were identified in rather small set {100, 150, 1.000, 1.500, 10.000, 10.500}. If psychology would not have influence on managing deposits, then the frequencies of each of these rounded and duplicated values would be much smaller. E.g. according to the Benford's Law first two digit test, frequency of first two digits combination starting with "10" is 5,6%. However in case of deposit payments there are 2,7% of payments starting with digit "1" that fall into set {100, 150, 1.000, 1.500, 10.000, 10.500}. So, only 6 values represent almost 3% of payment transactions starting with digit "1". That deviation is result of psychology factors that influence creation of deposit payment transactions. It may be stated that deposit transactions follow the same logic as some other payments and withdrawals for example ATM payments and withdrawals. The only difference is that ATM transactions are much smaller in amount.

So called currency exchange transactions participated in 6% of transactions starting with digit "1". Additional check on set {100, 150, 1.000, 1.500, 10.000} was performed and it was noticed that there are 22.656 exchange currency transactions which payment amounts are member of that five-element set (Table 16). That is 71% of all exchange currency transactions starting with digit "1".

amount	no of records
100	16.549
150	2.733
1.000,00	2.483
1.500,00	627
10.000,00	260
total:	22.652

Table 16. Specific rounded and duplicated payments amounts (currency exchange)

Rounded and duplicated values of currency exchange transactions considerably participated in deviation of digit "1" according to Benford's Law. When duplicated and rounded values are compared to surplus of transactions with first digit "1" (totalling 39.727) it is noticeable that they participated in surplus with more than 57%. If number of rounded and duplicated banking deposit (15.729) and currency exchange transactions (22.652) is summed it is obvious these two types of payments, which are under strong psychological influence of bank customers, almost equalled total surplus of transactions with first digit "1" (38.385 vs. 39.727). It may be concluded that psychological influence caused deviation of first digit Benford's Law distribution for transactions starting with digit "1" and that in this audit phase there is no evidence of any fraud, error or omission.

The similar analysis was performed for transactions with first digit "5" which was also in significant surplus in comparison to Benford's Law distribution. First step of analysis was based on summarization method where aggregation base attribute (column) was code of payment purpose and summarization function was count of records where only records starting with digit "5" were included. Summarization method resulted in grouping according to each unique payment purpose. For each group, number of actual transactions was counted. It was found that significant surplus of transactions having starting digit "5" in payment amount are following payment types:

- banking deposits (code of payment 870) - in total 26.018 records which is 16% of all records starting with digit "5"

- buying and selling of currency (currency exchange transactions, code of payment 912) - in total 17.018 transactions which is 10% of all transactions starting with digit "5"

It may be assumed if these two payment types did not have such significant surpluses, the Benford's Law first digit test would not indicate excess of 24.822 records (deviation of 17,96% from expected frequency) starting with digit "5" (Table 14). So, these payment types deserve additional attention and explanation.

As it is already explained previously, number clustering is usual with individual payments related to deposits. Further investigation shown that considerable rounding and duplication appeared in this particular case (Table 17):

amount	no of records
50	1.802
500	5.551
550	379
5.000,00	2.046
50.000,00	639
total:	10.417

Table 17. Specific rounded and duplicated payments amounts (deposits)

Data in Table 17 shows that 5.551 payment messages with amount 500 in original currency resulted in deposit or withdrawal from the bank i.e. related to deposit type of payment. Total of 10.417 rounded and duplicated payment amounts were identified in rather small set {50, 500, 550, 5.000, 50.000} which is 6,4% of payment transactions starting with digit "5". As with deposit payments starting with digit "1", significant clustering is result of psychology factors that influence creation of deposit payment transactions.

Currency exchange transactions participated in 10% of transactions starting with digit "5". Additional check on set {50, 500, 550, 5.000, 50.000} was performed and it was shown there were 15.937 exchange currency transactions which payment amounts are member of that chosen set (Table 18). That is 94% of all exchange currency transactions starting with digit "5".

amount	no of records
50	11.564
500	3.855
550	164
5.000,00	321
50.000,00	33
total:	15.937

Table 18. Specific rounded and duplicated payments amounts (currency exchange)

Rounded and duplicated values of currency exchange transactions significantly participated in deviation of digit "5" according to first digit Benford's Law. When duplicated and rounded values of currency exchange transactions are compared to surplus of transactions having first digit "5" (totalling 24.822) it is noticeable that currency

exchange transactions participated in surplus with more than 64%. If number of rounded and duplicated banking deposit (10.417) and currency exchange transactions (15.937) is summed it is obvious these two types of payments, which are under strong psychological influence of bank customers, almost equalled total surplus of transactions with first digit "5" (26.354 vs. 24.822). It may be concluded that psychological influence caused deviation of first digit Benford's Law distribution for transactions starting with digit "5" and that in this audit phase there is no evidence of any fraud, error or omission.

Since after applying steps 4 and 4.1 of CAISAM it could not be concluded that frauds, omissions or errors in business process exist (step 5 of CAISAM), it should be again tested if audit sample is relevant and complete (steps 4.2 and 4.3). This step is important, although it was already performed (steps 2 and 2.1) because already after the Benford's Law first digit test (step 3 and 3.1) and additional analysis of data because deviation existed (steps 4. and 4.1) auditor surely gained supplementary knowledge on data an business which can be used in re-checking of completeness and relevance of audit sample. Also, as it is noted in chapter 7.2, audit sample could be narrowed down to relate it with concrete business process and/or entity.

Summarization was performed according to month-year period of transaction date and bank that issued or received payment transaction. So, aggregation base attributes were month-year and bank code while summarization function was count of records:

month/year	no of banks	no of transactions
2-2008	35	525.662
3-2008	35	523.846
4-2008	35	695.803
	total:	1.745.311

Table 19. Summarization based on month-year period and bank code

Further analysis checked if each bank reported all codes of payment purpose (payment types). Analysis results were correct and according to expectations, so it was finally concluded audit sample is complete and relevant. According to CAISAM, after this second check of audit sample, there is no need for further check on its completeness and relevance.

The next step in CAISAM is the second digit Benford's Law test (step 6). It shown that digit 0 on second position in amounts appears significantly more often than it should according to Benford's Law - for more than 150% (Table 20).

d	fo	fs	fs-fo	Po	χ^2	Z
0	208.878	532.141	323.263	154,76	500.288	753,85
1	198.774	137.669	-61.105	-30,74	18.784	145,60
2	189.928	144.835	-45.093	-23,74	10.706	109,60
3	182.088	131.357	-50.731	-27,86	14.134	111,16
4	175.069	130.741	-44.328	-25,32	11.224	111,19
5	168.732	207.378	38.646	22,90	8.851	83,88
6	162.968	114.398	-48.570	-29,80	14.476	149,48
7	157.693	111.087	-46.606	-29,55	13.774	159,71
8	152.837	113.449	-39.388	-25,77	10.151	153,60
9	148.347	122.256	-26.091	-17,59	4.589	131,21
	Total:	1745311		43,12	606.977	

Table 20. Second digit (d) analysis of amounts in original currency payments

Digit 5 also appears significantly more on second position. It is noted that positive deviation is larger than 22%. This finding shows amounts are more often rounded on 0s and 5s than expected according to Benford's Law. It may be observed that business entities and individuals pay amounts (or get paid), deposit or withdraw and transfer or exchange money in rounded numbers more often than it could be expected according to Benford's Law. This is of course possible and again not immediate proof of errors, misstatements or frauds. It is also visible that all remaining second digits (1-4 and 6-9) have significant relative deficiency which is in fact result of excess in digits 0 and 5 on second position in numbers.

Since second digit "0" had the largest deviation it deserved more audit attention. Summarization method was executed including only payment transactions with digit "0" on second position in original payment amount. Code of payment purpose was aggregation base attribute and count of records as a summarization function. Summarization resulted in 91 different payment purposes. However, the following payment purposes had the most issued payments:

code of pp	description	no of transactions	% of transactions
870	banking deposits	84.771	15,93
912	currency exchange	63.492	11,93
340	financial service fees	45.312	8,52
110	payments for goods	43.586	8,19

Table 21. The most frequent payment purposes (“code of pp”) with digit "0" on 2nd position in payment amount

During analysis in steps 4. and 4.1 it was shown that amounts related to banking deposits and currency exchanges are often reflection of psychology. It was concluded that deviations of the Benford’s Law first digit test performed on whole audit sample resulted from deviation in amounts in transactions of these two payment purposes. Additionally, since in tables 15, 16, 17 and 18 it was observed that both “0” and “5” repeated in extremely high frequencies in amounts starting with digit “1” it may be concluded that banking deposits and currency exchange amounts drastically influence high frequencies of second digits “0” and “5”.

Consequently, further analysis must be performed for financial service fees (code of payment purpose 340) and payments for goods (code of payments for goods 110). Table 22 is a result of summarization according to payment amounts which are member of a set {10; 20;30;40;50;60;70;80;90;100;200;300;400;500}. That set is used as aggregation base attribute, while count was used as summarization function.

amount	no of records
10	26.974
20	4.226
30	3.687
40	754
50	2.313
60	193
70	254
80	318
90	200

100	938
200	182
300	153
400	53
500	52
total:	40.297

Table 22. Summarization of payments with purpose code 340 and specific amount set

According to explanation of properties for conformance of number set to Benford's Law (chapter 6.3), number series should not have defined minimal and maximal values. Also, observed number set should not have cut-off values causing discontinuation. As it is known from the experience, banking policies are very often set with minimum and maximum fee, while fees in between these ending values are set with certain cut-off values. From example shown in Table 22 it is clearly noticeable that fees have a number of repeating values which probably result from banking policies concerning fees and their breaking values. So, fee amounted to 10 in original currency is represented in 60% (appears in 26.974 cases) cases of financial service fees. Also, 40.297 fee amounts are in fact result of rounding and duplication. So, it may be said that financial fees will not follow Benford's Law because underlying fee amounts usually have minimum, maximum and cut-off values. Furtherly, a number subset which does not follow Benford's Law may cause discrepancy for whole observed number set. Since fee values from rounded and duplicated set shown in Table 22 participate with 12,5% in whole surplus of amounts with second digit "0" (323.263) it may be stated that fee amount subset significantly implicate deviation of second digit Benford's Law distribution.

Further analysis of payments for goods should also be performed (code of payment purpose 110). Table 23 is a result of summarization according to payment amounts which are member of a set {[10..100]mod10=0, 500,1.000,2.000,3.000,4.000, 5.000,6.000, 7.000,8.000,9.000,10.000,20.000,30.000,40.000,50.000}. That set is used as aggregation base attribute, while count was used as summarization function.

amount	no of records
[10..100]mod10=0	764

500	410
1.000,00	1.018
2.000,00	1.519
3.000,00	1.377
4.000,00	967
5.000,00	2.055
6.000,00	709
7.000,00	524
8.000,00	488
9.000,00	305
10.000,00	2.598
20.000,00	1.186
30.000,00	638
40.000,00	387
50.000,00	536
total:	14.867

Table 23. Summarization of payments with purpose code 110 and specific amount set

Total of 14.867 payment for goods transactions are in fact result of rounding and duplication which is 34% of this type of transactions with second digit “0”. Also, transactions shown in Table 23 participate with 5% in surplus of all payment transactions with second digit “0” (323.263). The question that must be answered is why payments for goods are deviated in such manner and why there are so many rounded and duplicated values. Firstly, it should be noted payment for goods are usually transacted in a few annuities. Respectably often, annuities are not result of calculation but rounding. So payee may agree with payer certain dynamic and rounded amount payments. Those roundings may be a cause of deviations. Probably it is true that roundings based on agreements between beneficiary and buyer caused deviation in above explained case. More on this issue can be found on page 146 when deviations in the first two digits test are analyzed.

Second digit "5" also had the positive deviation so it earns additional analysis. Execution of summarization method including only payment transactions with digit "5" on second position in original payment amounts resulted in Table 24. Code of payment purpose was aggregation base attribute and count of records was a summarization function.

Summarization resulted in 91 different payment purposes. However, the following payment purposes had the most issued payments:

code of pp	description	no of records	% of transactions
870	banking deposits	34.846	16,80
110	currency exchange	25.205	12,15
340	financial service fees	20.216	9,75
912	payments for goods	9.025	4,35

Table 24. The most frequent payments purposes (“code of pp”) with digit "5" on 2nd position in payment amount

As it can be observed, 43% of all payments having second digit “5” is belonging to banking deposits, currency exchange, financial service fees and payment for goods. It was already explained that all of these types of payments may be:

- negotiated and agreed between parties while agreement does not have to correspond to any calculation but to number invention which is under strong influence of psychology (payments for goods)
- result of psychology and number simplification of bank’s customer (banking deposits and currency exchange)
- result of minimum, maximum and cut-off values which break sequence continuity of number set (financial service fees)

Consequently, all of these payment types are subject to rounding and duplication. Such rounding and duplication reflects in significant surplus of certain second digits as it is visible for second digit “5” in payment messages. In addition, analysis shown that more than 92% of second digit “5” surplus (38.646) was inflicted by following rounded values:

- values divisible by 5 but not with 10 between 10 to 100; and divisible by 50 but not with 100 from 100 to 500 - for financial services fees;
- values from set {150,550,1.500,15.000,25.000} for banking deposits, currency exchange and payments for goods.

Outcome of the summarization based on above mentioned parameters is displayed in Table 25.

code of pp	no of records
110	5.864
870	9.902
912	8.647
340	8.893
total:	33.306

Table 25. Rounded values of selected codes of payments with second digit “5”

As it is shown in Table 25 there are 33.306 rounded values for selected codes of payments. That is 86% of surplus amount for all payments with second digit “5”. If these rounded and duplicated amounts would be distributed over all second digits, surplus would be considerably smaller and possibly even insignificant.

Finally, it is shown that second digits positive deviations are not result of an error, mistake or fraud, but are result of a normal business conduct. These deviations are simply outcome of psychological influence when bank customers deal with certain types of payments (bank deposits, currency exchange transactions), agreements or payment contracts between payer and payee (payment for goods transactions) and result of business rules (financial service fees transactions).

According to CAISAM, the first two digits Benford’s Law test is the next method that must be applied on data (step 9). It was executed on all payments from audit sample. The first two digits test shown significant positive deviation of all first two digits divisible by 10. Deviation ranged from 53% for digits “90” to almost 430% for digits “50”. In Figure 10 percentages of deviation of actual from expected frequency are shown for two digit combinations (10 - 99). Significant deviations can be easily spotted. Also, it is obvious that there are positive deviations for some digits divisible by 5 and not by 10 (15, 25, 35, 65, 75).

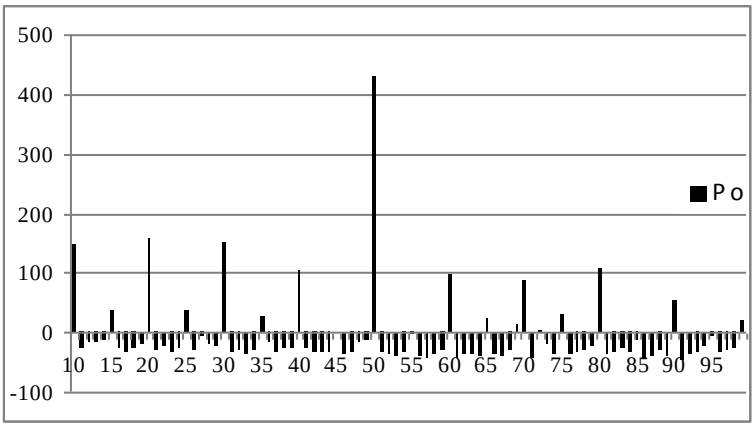

Figure 10. Frequency deviation from Benford's Law for first two digits for all payments in original currency

In absolute value, there were 179.205 amounts in original currencies beginning with digits "10" which is 148% more than frequency according to Benford's Law. Also, this is more than 10% of all amounts i.e. observed transactions. According to first two digits Benford's Law, only 72.243 transaction amounts should begin with digits "10" which is probability of 4,14%.

Deviations of numbers starting with digits "50" are the largest. In absolute value, there were 79.325 amounts in original currencies beginning with digits "50" which is almost 430% more than frequency according to Benford's Law. However, this is only 4,5% of all amounts i.e. observed transactions. According to Benford's Law, only 15.010 transaction amounts should begin with digits "50" which is probability of 0,86%.

This characteristic was examined in more details by searching for rounded numbers starting with "10". It was shown that there are 127.593 amounts in original currency which are members of set {10, 100, 1.000, 10.000, 100.000, 1.000.000, 10.000.000} which is more than 7% off all transactions. That shows that too many transactions had amounts from above defined set.

Also, concerning rounded numbers starting with "50" search shown that there are 70.066 amounts in original currency which are members of set {50, 500, 5.000, 50.000, 500.000, 5.000.000, 50.000.000} which is 4% of all transactions. That also shows that too many transactions had amounts from above defined set.

Further, different type of payments participating in surplus were searched for and discovered that important percentage of rounded transactions and transactions starting with digits “10” or “50” are again banking deposits, currency exchange, financial services fees and payments for goods. The same payment purposes participated in significant surpluses when first and second digit Benford’s Law were applied (steps 3 and 6). For example number set of amounts in currency exchange has 30.448 more amounts beginning with “10” than it should be expected according to Benford’s Law which is 353% difference. Also, there are 25.142 more occurrences of amounts of same type starting with digits “50” which is 14 times more than Benford's Law distribution for those digits (1.792). These deviations can be explained by psychology or custom in exchanging (buying or selling) rounded amounts or amounts starting with digits “10” or even more with digits “50”. As it is already stated, these deviations can be explained by custom in number creation and influence of psychology when inventing numbers. For example, it is more usual to exchange (sell or buy) 100 EUR for kunas then to exchange 98 EUR or 112 EUR.

However, it was noticed that also currency transfers to Croatia and to abroad constituted surpluses for digits “10” and “50”. Transfers of money from abroad to Croatia and from Croatia to abroad related with worker’s payments to their families, transfers connected with migration abroad or to Croatia, payments for memberships in organizations and associations and transfers of government funds from abroad that begin with digits “10” appeared in 92% more values than it should be expected by Benford’s Law distribution. However, majority of these transactions are money transfers initiated by workers temporarily or permanently working abroad who support their families living in Croatia through money transfers.

This deviation can be again explained by custom in number creation and psychological factors. Croatian workers temporarily or permanently working abroad will more often than it is expected by Benford’s Law (and uniform) distribution send money amounts in rounded numbers or numbers beginning with digits 10 or 50 (e.g. 500 or 1.000 EUR) to their families residing in Croatia.

All other payment types showed no discrepancy from Benford's Law first two digits test.

In previous tests, quite reasonable explanation of positive deviation surpluses of certain digit combinations was given for banking deposits, currency exchange, financial service

fees and money transfers. Deviations of amounts of these payment types were explained by psychology factors, customs in number creation, minimum/maximum values allowed and cut-off values causing discontinuance. Payments of goods were also identified as cause of positive significant deviation. It was commented that was outcome of the way payment amounts were created: often payment annuities amounts are agreed upon and again influenced by psychology and customs in number creation. However, this type of payment deserves some additional analysis.

It is skipped back to step 3 so the first digit Benford's Law test of payment amounts in original currency is performed. The results are shown in Table 26.

d	fo	fs	fs-fo	Po	χ^2	Z
1	74.123	74.540	417	0,56	2,34	1,83
2	43.359	43.656	297	0,68	2,03	1,57
3	30.764	30.558	-206	-0,67	1,38	1,26
4	23.862	23.797	-65	-0,27	0,18	0,45
5	19.497	21.429	1.932	9,91	191,45	14,42
6	16.484	15.428	-1.056	-6,41	67,70	8,52
7	14.279	13.464	-815	-5,71	46,57	7,03
8	12.595	12.067	-528	-4,20	22,17	4,83
9	11.267	11.293	26	0,23	0,06	0,25
	Total:	246.232		3,18	333,89	

Table 26. First digit (d) analysis of amounts in original currency payments for goods

Deviations for first digits 1,2,3,4 and 9 are not significant. This is obvious even for very sensitive chi-square and Z-statistics tests. Z statistics test falls within cut off value (1,96). Also, chi-square values for mentioned digits are not the cause for excessing cut off value (15,507). There is significant surplus of amounts starting with digit 5 (almost 10%) and deficit of amounts starting with digits 6, 7 and 8. Deficits can be explained by surplus for digit 5, i. e. digit 5 surplus caused deficits in some other digits. Since value for χ^2 (333,89) is still above cut off value (15,507), it must be concluded that this number subset does not follow Benford's Law. However, it can easily be noticed that deviations are significantly lesser than with previously mentioned types of messages. Since only significant surpluses should be furtherly investigated, auditor should focus only on first digit 5. This deviation

again can be explained by customs in number creation as well with contract terms which is explained in more detailed manner further in the text.

The first two digits Benford's Law test on payments for goods transactions shown significant deviation of all first two digits divisible by 10. Deviation ranges from 26% for digits 90 to 135% for digits 50. In Figure 11 percentages of deviation of actual from expected frequency are shown for two digit combinations (10 - 99). Significant deviations can be easily spotted. Also, it is obvious that there are positive deviations for some digits divisible by 5 and not by 10 (15, 25, 75). Also, there is negative deviation for digits 85.

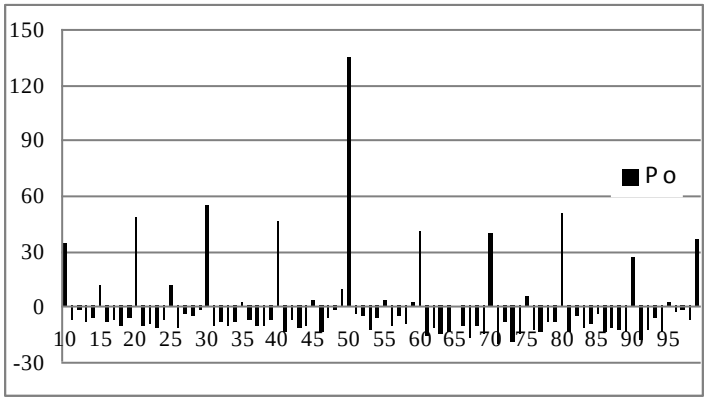

Figure 11. Frequency deviation from Benford's Law for first two digits of original currency payments for goods

Additional investigation of payments from abroad for goods exported from Croatia to abroad was performed.

D	Fo	fs	fs-fo	Po	χ^2	Z
1	19.540	19.514	-26	-0,13	0,03	0,22
2	11.430	11.429	-1	-0,01	0,00	0,01
3	8.110	7.951	-159	-1,96	3,10	1,88
4	6.290	6.413	123	1,95	2,39	1,63
5	5.140	5.316	176	3,43	6,06	2,57
6	4.345	4.288	-57	-1,32	0,76	0,91
7	3.764	3.763	-1	-0,03	0,00	0,02
8	3.320	3.234	-86	-2,60	2,24	1,53
9	2.970	3.001	31	1,04	0,32	0,58
	Total:	64.909		1,39	14,91	

Table 27. First digit (d) analysis of amounts in original currency payments from abroad for exported goods

According to Z-statistics test, only significant deviation appeared for digit 5. The same can be concluded for MAD test. Chi-square test shown that observed subset of payments for goods follows Benford's Law distribution.

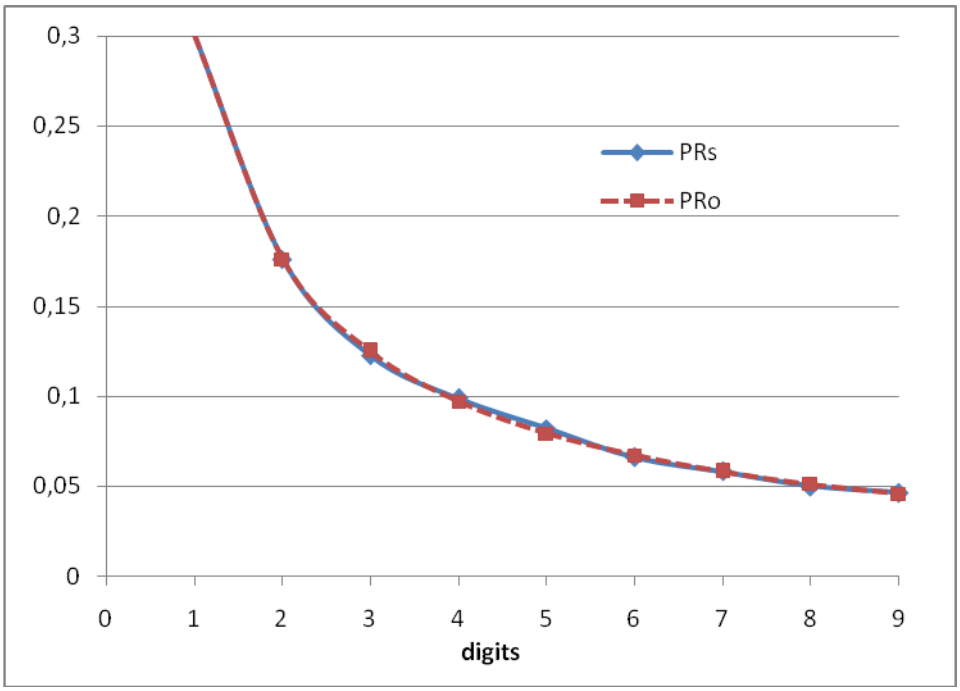

Figure 12. Actual (PRs) and Benford's Law proportions (PRo) of original currency payments from abroad for goods

Figure 12 serves as useful visualization of actual and expected (Benford's Law) proportions of payments from abroad for goods in original currency. It is visible that deviation is considerable only for digit "5". However, all conformance criteria (MAD, Chi-square, Z-statistics) are within acceptable limits so it may be stated that amounts of payments from abroad for goods conform to Benford's Law first digit distribution. Usually, when focus is given to specific subset of data, in this case payments from abroad for goods exported from Croatia, deviations from Benford's Law distribution are significantly smaller. Following table shows differences in deviations for entire set of payments for goods and subset related to payments from abroad for goods exported from Croatia.

transactions	MAD	Chi-square	Z-statistics (no of exceeding digits)
payment for goods – entire set	3,18	333,89	4
payment for goods – from abroad	1,39	14,81	1

Table 28. Comparison of deviations between payments for goods

Generally speaking for all previously performed investigations of payments for goods, total amounts on invoices that equal to value of corresponding contracts for goods may not be deviated in the same manner, i.e. only single payment amounts may be deviated according to contract terms. Business entities may agree to pay amounts in more than one rate, i.e. according to contracted terms and/or subsequent arrangements and to apply payment method which will more often than expected according to Benford's Law produce rounded numbers or numbers starting with multiplies of 5 (and 10) for payments. For example, although contracted value was 42.342 EUR, business entities (buyer and seller) might have agreed on five payment annuities. First annuity could be 10.000 EUR, as well as annuities resulting in second through fourth payment. Last, fifth payment could have covered the rest of contracted value (2.342 EUR). That way clustering of rounded values is easily explained. However, to audit and proof this assumption, certain number of business entities should be chosen and their contracts and defined payment methods checked. Identification of business entities is performed in each payment transaction for goods, so this is not impossible task for state authorities. However, this is beyond the scope of this paper and also beyond the capabilities of author.

For purpose of audit it is possible to identify individual payer or payee and then perform Benford's Law tests on its received or ordered payments. If tests against Benford's Law significantly deviate, auditor may perform some additional tests only for certain digits which deviate from Benford's Law frequencies in order to check against fraudulent or erroneous activity. These tests could, for example, include:

- rounded amounts, amounts starting with multiplies of 10 or 100
- counting frequency for each amount – searching for multiple occurrences (number duplication) of the same amounts (especially in short period of time)
- rounded and duplicated amounts on very same day

- rounded and duplicated amounts for the same type of payments in specific period of time
- rounded and duplicated amounts in specific or different banks
- amounts slightly below certain threshold – this can be done to check if payer or payee wanted to evade entering certain tax limits or additional checks by authorities (for example, if person transfers amount above 100.000 kunas)
- amounts slightly greater than certain threshold – sometimes business entities with performance (money spent, invested, bought etc.) above certain limits may get special status in their relationships with state authorities, banks or other business entities
- multiple payments of same type paid same day (or in short time interval) with sum above or below certain threshold

Also, it is advisable to choose among certain business entities which have the largest number of rounded and duplicated values or values slightly lesser or greater than certain threshold and perform detailed audit.

These tests can be quite easily performed by use of computer assisted auditing tools (CAAT). CAATs have a number of predefined auditing methods to ease data examination and conclusions brought by auditor.

According to CAISAM, one more Benford's Law test must be executed. It is the first three digits test (step 12). This test takes into consideration 900 first three digit combinations. After this test was performed on payment transaction amounts, it was noted that all three digit combinations divisible by 50 had significant positive deviations. Table 29 contains all first three digits combination that had positive deviations.

D	fo	fs	fs-fo	Po	χ^2	Z
100	7.542	132.786	125.244	1.660,59	2.079.781,22	1.445,27
150	5.036	37.595	32.559	646,46	210.478,55	459,44
200	3.780	74.374	70.594	1.867,33	1.318.212,04	1.149,38
250	3.026	24.854	21.828	721,38	157.464,55	397,16
300	2.522	49.283	46.761	1.853,81	866.854,47	931,72
350	2.163	17.097	14.934	690,59	103.135,25	321,35

400	1.893	29.391	27.498	1.452,95	399.538,49	632,43
450	1.683	8.582	6.899	410,07	28.292,33	168,28
500	1.514	71.158	69.644	4.598,60	3.202.630,70	1.790,37
550	1.377	6.275	4.898	355,74	17.424,40	132,05
600	1.262	19.171	17.909	1.418,80	254.088,59	504,26
650	1.165	5.166	4.001	343,35	13.736,48	117,24
700	1.082	15.848	14.766	1.364,61	201.498,05	449,03
750	1.010	8.344	7.334	726,16	53.257,02	230,84
800	947	15.114	14.167	1.496,19	211.966,97	460,52
850	891	3.949	3.058	343,10	10.491,26	102,45
900	842	9.214	8.372	994,65	83.274,81	288,64
950	797	3.549	2.752	345,04	9.494,05	97,46

Table 29. Selected results of the first three digits Benford's Law test

Also, much larger surpluses could have been noticed on first three digits divisible by 100. That is in conformance with the first two digits test which also shown larger surpluses of all first two digits divisible by 10 than of first two digits divisible by 5 and not by 10. Of course, since the first three digits test is more focused (has 10 times more digit combinations than the first two digits test) it can express more details on audit sample.

Further examination i.e. summarization of transactions with amounts starting with first three digits contained in table 29 according to aggregation base attribute code of payment purpose and count aggregation function shown that banking deposits, currency exchange, financial service fees and payments for goods transaction were cause of these significant discrepancies from Benford's Law distributions.

Earlier in the text it was explained that these four payment types caused deviations since their amounts are:

- under strong influence of psychological factors in number creation (banking deposits and currency exchange amounts),
- outcome of difference between contracted values and rounded and duplicated annuity amounts (payment for goods),
- influenced by minimum, maximum and cut-off values (financial service fees).

So, it may be stressed that on the basis of the first three digits Benford's Law test no fraud, error or omission was found in the audit sample (step 14).

At final of CAISAM, it must be concluded on audit process (step 15). As it was stated during previous methodology steps, there were no significant findings that could prove existence of fraud, omission or errors in business conduct. However, it was noticed that some deviations from Benford's Law exist in payment messages data. Those deviations which were outcome of number rounding and duplications were explained by psychology of payer in creation of payment amounts, agreed dynamic of payments and customs in number invention as well as with fact that some number sets are simply not in accordance with Benford's Law.

It is worth to write a few observations on practical usefulness of conformity tests we used (chi-square, Z-statistics and MAD) in auditing environment.

A problem with chi-square test in auditing environment, which is of course different than statistic environment, is its excess power problem. When the data set becomes significantly large, chi-square test will almost always be higher than the cut of values which could force auditor to make a non conformity conclusion about observed frequencies. The problem usually occurs for data sets larger than 10.000 observations which mean that small, even immaterial differences will result in conclusion that data set does not follow Benford's Law [17 , page 78].

In our investigation, when any individual value for Z-statistics exceeds 1,96 it may be concluded the difference is significant at 5% probability. To be more precise, there is only 5% probability that the difference is caused accidentally. However, this is still quite a big probability and such differences, caused by chance, are quite often in auditing. Z-statistics values are calculated for each digit separately. If we have 9 digits in focus (e.g. in the first digit test), each digit has 5% probability of having accidental Z-statistic greater than 1,96. Then, the chance that at least one of the nine digits will have Z-statistics out of limit is 37%. To furtherly emphasise importance of this, we may conclude that for audit purposes it is not enough to use only Z-statistics test in order to confirm whether data are Benford's Law compliant.

Chi-square and Z-statistics tests are too sensible in statistical sense for practical value in making audit conclusions. This is especially true when Chi-square tests are applied on large volumes data because tests are then even more sensible.

However, these tests can be used for narrowing down which digit(s), whose frequency deviations are out of cut off value in case of Z-statistics or cause sum of chi-square calculations moves out of boundaries, should auditor investigate by other auditing and data analysis methods. For example, if the threshold for payment transactions monitored by tax authorities is 50.000 kunas, then a surplus of two digit combinations of 49 for such transactions in certain bank will be very significant. It may suggest that persons and business entities having account with specific bank are splitting amounts in order to avoid threshold.

Also, if data simply does not conform to Benford's Law then many digits will have Z-statistics greater than 1,96. Also, many digits will cause sum of chi-square value is above limit (15,507 for 8 degrees of freedom with 5% significance). This kind of noncompliant data means that:

1. the data is fraudulent, or
2. the data sample is incorrectly extracted i.e. it is not representative, or
3. on the contrary to our assumption, the Benford's Law is simply not applicable to audited data

It is very important to bear in mind that usually only positive deviations have importance for auditors. So, all chi-square and Z-statistics values with negative deviations should not be in audit focus.

MAD is the average deviation between the Benford's Law frequencies and actual frequencies. The higher the MAD, the larger is average difference between actual and Benford's Law frequencies. One of very important advantages of MAD in comparison with chi-square is its independence of the size of data set. Also, auditors claim it is the easiest to understand and therefore most often used. Although there are still no strict and widely accepted cut off values for MAD, in [17, pages 118-122] some rules are set for creation of MAD limits. We conclude that MAD in combination with individual average deviations is appropriate goodness of fit technique which can easily be used for detection if data set conforms to Benford's Law. Also, individual average deviations (Po) can be used

as guidelines in data auditing. Each significant positive average deviation should be investigated in more details in order to conclude if deviations are outcome of errors, frauds, negligence or chance.

7.4 Evaluation of Developed Methodology

Business processes are supported and enabled by information systems. As a consequence of constant change and development of business processes information systems that support them tend to become very complicated and use enormous volumes of data. It brings the conclusion that often it is not possible to audit information system without computer assisted auditing. Although various methods for computer assisted auditing of information systems exist that are even supported by computer assisted auditing tools, there is need for development of unified methodology.

In chapter 7.2 such methodology (computer assisted information systems auditing methodology - CAISAM) was designed and based on Benford's Law tests. Four Benford's Law tests were chosen as a basis of methodology: the first, the second, the first two and the first three digits tests. From the very first step it is strongly focused on completeness and relevance of audit sample. In the practice, lot of audits were inadequate because of incomplete or non-relevant data. Surely, in order to choose adequate audit sample, auditor must have solid knowledge on business processes and data. Especially important is knowledge and capability of auditor to match data structures (tables and columns, relationships between tables) to business events and processes.

Methodology includes very efficient methods for checks of entire data set (the first and the second Benford's Law tests, stratification and summarization) on reasonableness, completeness and adequacy. Also, more focused Benford's Law tests (the first two and the first three digits) are provided and ways of their usage are explained very extensively. Methodology is strongly directed toward interpretation of Benford's Law tests results. According to results of tests, it gives guidance on further data analysis with other supporting methods: summarization, join, stratification, selection, rounded values and duplication checks.

Inputs, outputs and assessed strength of specific methods in all steps of developed methodology are presented in Table 30.

Step of CAISAM	Method	Inputs (I) and Outputs (O)	Strength
1. Data provision	selection	Rows of relational table (I) Rows of relational table satisfying WHERE clause criteria (O)	V
	join	Rows of two relational tables usually with at least one common attribute (I) Rows of newly formed temporary relational table satisfying join type and criteria (O)	P
2. AS check	selection	The same as in step 1.	V
	summarization	Rows and attributes of relational table, aggregation functions (I) Rows grouped on unique attribute values, aggregated on selected attributes with certain aggregation function (O)	V
	stratification	Rows and attribute of relational table, strata limits, mathematical functions (I) Data layers with counted and summarized rows together with calculated percentages for chosen attribute (O)	V
	join	The same as in step 1.	P
3. BL on AS	FDT	Attribute of relational table containing number values (I) 9 subsets for digits 1-9 with actual frequencies and corresponding deviations (O)	P
4. AS check FOE	selection	The same as in step 1.	V
	summarization	The same as in step 2.	V
	duplication	Rows and attribute of relational table (I) Rows grouped and sorted descending by frequency and descending by numeric value of chosen attribute (O)	P
	rounded	Rows and attribute of relational table	P

	values	(I) Rows grouped and sorted descending by frequency and descending by numeric value of chosen attribute (O)	
5. Conclude on FOE	selection	The same as in step 1.	V
	summarization	The same as in step 2.	V
	rounded values	The same as in step 4.	P
	duplication	The same as in step 4.	P
6. BL on AS	SDT	Attribute of relational table containing number values (I) 10 subsets for digits 0-9 with actual frequencies and corresponding deviations (O)	P
	FTDT	Attribute of relational table containing number values (I) 90 subsets for digits 10-99 with actual frequencies and corresponding deviations (O)	V
	FThreeDT	Attribute of relational table containing number values (I) 900 subsets for digits 100-999 with actual frequencies and corresponding deviations (O)	V

Table 30. Methods used in CAISAM

Abbreviation “FDT” stands for “First Digit Test”, “SDT” for “Second Digit Test”, FTDT denotes “First Two Digits Test”, while “FThreeDT” means “First Three Digits Test”. “BL on AS” means “Benford’s Law on audit sample”, i.e. specific Benford’s Law test applied on selected audit sample of data.

The column “Step of CAISAM” contains the short name of CAISAM step as described in chapter 7.2 within the model of methodology. The column “Method” contains each method that should be applied in each CAISAM step. “Inputs (I) and Outputs (O)” column includes inputs and outputs of each CAISAM method. The column “Strength” contains usability level of each method within certain step. In this notation, “P” stands for “powerful” meaning method is useful in certain CAISAM step and helps in improvement of the audit process. On the other hand, “V” stands for “very powerful” which means

method is very useful in specific step of CAISAM and significantly improves the audit process. Of course, usability of the same individual method may vary in different steps of CAISAM.

CAISAM leads auditor from less to more data focused steps which is very reasonable approach. That way, auditor gradually improves its knowledge of data and business rules that influence data creation. Conformance criteria for evaluation of conformity of data sets with Benford's Law distributions ensures the enhancement of auditor's focus on data subsets thus significantly improving further data examination process. It is shown how relatively simple methods like rounded values, duplication checks and summarization may be very effective in data analysis when combined within methodology.
Methods, steps, input and results of each method together with possible conclusions in practical situations are established. With such methodology, whole auditing process can be improved, become consistent, standard, comparable and executed faster with fewer resources.

Complex and data extensive audit was successfully completed by use of CAISAM in chapter 7.3.3. Methods prescribed by methodology were applied on real-world data and certain deviations were detected. These deviations were successfully analyzed by CAISAM and explained in details. Thus, methodology was proven efficient and useful in practical audit of information systems i.e. large data sets.

8. Improvement of Computer Assisted Auditing Tools Functionality and Auditing Quality

As companies and institutions use information systems to store and process constantly increasing amounts of data, the necessity grows for definition and use of auditing procedures in producing adequate risk assessment concerning data management. Computer assisted audit tools (CAATs) are becoming increasingly important tool in evaluation of the control mechanisms in more efficient course. Application of CAATs improves audit scope, completeness and consistency of data analysis. This all together leads to more effective operational i.e. information systems risk mitigation.

CAATs can be a source of a large proportion of the audit evidence developed on information systems and business activity audits, so the auditor must carefully plan, execute, document and report use of CAATs during the audit process. Guideline G3 of ISACA set of guidelines for effective information systems audit provides direction in applying CAAT [45]. Although this guideline is the most widely accepted in the auditing community and became de facto standard, in forthcoming chapters (8.1 to 8.3) a number of recommendations on additional improvement will be given.

No matter if CAAT is developed by auditor, by auditor's internal IT staff or by commercially oriented IT company, it is vital that the auditor obtain reasonable assurance of the integrity, reliability, usefulness and security of chosen CAAT. This must be assured by adequate testing and review of CAAT documentation. Of course, this evaluation must be done before CAAT is used in any actual audit. The extent of testing is dependent on the commercial availability and broadness of the CAAT usage. Commercially produced and widely available CAAT should also be tested but not so extensively as internally developed tools. Internally developed CAAT must be thoroughly reviewed and tested in accordance to one of standard software development methodologies to ensure CAAT functions as planned.

8.1 Audit Phases and Necessary Characteristics of Computer Assisted Auditing Tools

Computer assisted auditing tools may be:

- Developed by internal programming staff or by outside programmers with audit department supervision;
- Purchased generalized audit software, e.g., audit packages offered by commercial audit firms or software vendors;
- Developed by IT auditors themselves;

According to [38], whatever is the source of CAAT, it must remain under the rigid control of the audit department. For this reason, all documentation, test material, source listings, source and object program modules, and all changes to such programs, should be strictly controlled. In installations using advanced software library control systems, audit object program versions should be protected with passwords. This is acceptable if the auditors retain control over the documentation and the appropriate job control instructions necessary to retrieve and execute the object program from the libraries where it is stored. Computer programs intended for audit use should be documented carefully to define their purpose and to ensure their continued usefulness and reliability.

Furtherly, there are certain characteristics in each auditing phase that should be implemented when using CAAT or within CAAT. In chapters 8.1.1 to 8.1.4 some important characteristics of necessary audit steps are explained in more details.

8.1.1 Audit Planning

The purpose of this phase is development of an audit plan. During the audit planning process, the auditor must evaluate the need and advantages of manual techniques and CAATs. Important factors in determining whether to use CAATs or manual approach are [45]:

- Computer knowledge, expertise, and experience of the auditor
- Availability of suitable CAATs and IT facilities
- Effectiveness of using CAATs over manual techniques
- Time constraints

- Integrity of the information system and IT environment; volumes of data
- Level of audit risk

Since large volumes of data become very often as well as significant complexity of business conduct, usually the CAATs will be the only option that is practical and efficient enough.

The main steps auditor must address when plan for the implementation of CAAT cover the following:

a) Understanding of business conduct

It is very important that auditor using CAATs understands the business being audited. Of course, this is the most important prerequisite even if no CAAT is used but ordinary audit is performed. The aim is to map business activities to computer assisted audit methods. After auditor identifies certain risks in business conduct, he/she must define how audit methods will be performed and on what data. Clear objectives of the CAAT's use in specific audit process must be defined. It must be formulated what methodology will be used and what data will be audited. In chapter 7 very useful methodology is explained in details.

During this phase, auditor should start cooperation with customer being audited (the auditee). On the first meeting, auditor must explain to auditee planned activities. Also, the auditee should put forward his expectations and view of management on his business activities and governance. In addition, the auditee must perceive the purpose, scope, objectives, his/hers role or the role of auditee's IT experts in the usage of CAAT's in auditing process. Defining clear anticipations of the CAAT role should be communicated. Auditor should gather as much information as possible in order to further get knowledge on auditee's business. Especially, auditor must be focused on the risks in client's business. He/she must learn more on information system and information technology as well as their operating procedures and management, administrative and technical controls.

b) Understanding of data

However, when CAATs are being used, crucial component is mapping of business activities and business view of data (through documents, application forms, application reports etc.) to data structures in information systems. That means auditor must get

knowledge of database structures and their relations to client's perception, views and interpretations of data. It must be stressed database structures and client's views of data are usually very different. The task of data mapping may be extremely complex, especially if existing data structures are not sufficiently documented. Then, auditor must spend additional resources in order to learn about data and its relation to business. This task is strongly related to process of understanding the business.

Furthermore, the accessibility and availability of the organisation's data must be identified. It must be clear what procedure must be undertaken in order to export the data from production database, who will grant the access rights, who will give the authorization for extraction, what will be the output format and how data will be checked for completeness and correctness. Auditor must clearly define which data should be extracted from database. In order to accomplish that task, data tables must be clearly identified, together with precise selection criteria, eventual joins and summarization definition. The use of these methods is explained in more details in chapter 7, however prerequisite for their appropriate use is the detailed knowledge of data already in the planning stage.

It is obvious that during the data extraction, i.e. creation of audit sample, some sensitive or confidential information and data can be accessed. Of course, that information and data must stay confidential. The auditor must be informed and clearly understand auditee's information and data classification together with their handling policies. Auditor is bound by non disclosure agreement which means he/she is obliged not to relieve any information or data to third parties. However, the auditor must also handle and safeguard the data and information with an appropriate level of confidentiality and security. In doing so, the auditor must use at least the level of confidentiality and security required by the auditee owning the data and any relevant legislation. The auditor must consult auditee if it is not clear which data is confidential and especially if mode of its protection and handling is not appropriately established.

Output format requirements of extracted data must be established. Since extraction of data from production environment is usually executed by the IT personnel, auditor must formulate details of extraction format. Examples of file formats are ASCII text delimited, ASCII text fixed width, Excel, dBASE, Access, XML etc. Auditor also must define columns and their data type. For some data types, it is necessary to define formats. So, for numeric column it is needed to state if numbers will contain decimal point or comma,

whether numbers will have thousands separators and how negative numbers will be represented (minus sign before or after the number). Also, for date columns, date format type must be defined. Examples of date format types are various and their definition by auditor must be based on D (day), M (month) and Y (year) convention.

Transactions in production databases are often only stored for a limited time, usually because operational management issues and system performance. So, the auditor must clearly define for which time frame he/she requires the data. If all data needed is not stored on production environment, auditee's IT personnel will probably have to recover data from backups. That process can be time consuming, so auditor has to take it into account when developing auditing plan.

Also, business entities usually have strict rules concerning execution of tasks which are not directly related to everyday operation. That means that data extraction activities should be arranged well in advance in order to minimise the impact on the business' production platform.

Even when CAAT is used to directly extract data from databases, the auditor must verify the data are correctly extracted. Also, when choosing CAAT for audit process, auditor must check correctness of CAAT's extraction feature.

c) Auditing team set up

Very rarely auditing activity of any kind will remain on one expert. As it is already stated, volumes of data may be very large, business complexity may be significant, so interdisciplinary knowledge of business conduct, information systems and technology is required. The objective of this planning step is to form the auditing team, to communicate it among team members and agree on duties of each audit team member. Team members may include experts out of auditor's organization, audit managers who will approve and sign the audit report, staff auditors who will perform audit work and any additional specialists indispensable for getting the work done. As it is emphasized in [30], the meeting for audit team set up must be held to communicate all open matters including client requirements and deliverables by the audit team, level of involvement of each audit team member, their roles and responsibilities. Very important point of this meeting should be the matters of business understanding, data understanding and most effective process of information compilation. In the case of auditee continuance, a review of prior audits should

be identified and analysed. That way it will be easier to assess scope of new audits and to double check gathered data.

d) Knowledge of the information system and technology

Apart from knowledge of data, auditor must determine processing environment from which data will be exported. Usually this is not a trivial question, since businesses have few processing environments. Very often there are at least development, testing, production and reporting (data warehousing) environments. These environments may be supported by different databases, applications and hardware equipment. Also, auditor must also define how gathered data will be verified. In some business entities auditor is permitted to connect the system and to extract data together with IT personnel. However, usually it is not accepted, so auditor must perform additional checks on data received as an audit sample. How these checks of audit sample should be performed is explained in chapter 7.2.

e) Selection of methodology on which CAAT will be based

A very useful methodology for computer assisted information systems auditing is developed, explained and verified in chapter 7. That methodology is largely based on Benford's Law, although it assumes use of handful additional methods. However, auditor needs to define methods, their sequence and mutual relationships, input and output values from each method as well as flowchart of methodology. Of course, CAAT tool that will be used must support chosen and established at least key aspects of methodology. Auditor must bear in mind that those methods not supported by CAAT have to be supported by other software products or additional programming. It can be quite cumbersome and inefficient, so auditor should insist on coverage of as much methodology steps and methods with one CAAT as possible. Otherwise, audit activity could become extremely time consuming and require more experts (for each additional software or additional programming modules). Since data must be moved from CAAT tool to other specialized software product or programmed modules, data mergers become mandatory. That inevitably brings additional complexity to data analysis. Switching from one tool to another together with data transformation and transfer between each tool also yields additional risks to audit process. Conclusion is that ideal situation is when only one CAAT is used in audit process.

8.1.2 Audit Execution

The audit execution is a central step in audit conduct. It includes actual use of CAAT and audit methodology. The actual audit execution based on computer assisted information systems auditing methodology is described in chapter 7.3. Although that methodology enables auditor of adequate audit execution, it is surely not the only one audit may be executed. Obviously, a number of various methodologies could and would be developed in the future. Except the methods explained in chapter 5, the question that should be answered is what methods should be incorporated within CAAT. According to a practical view on CAAT efficiency the list of indispensable CAAT methods follows. It clearly shows variety of methods CAAT should support as well as plenty of approaches auditor could consider in execution phase of audit conduct, respectively to type of work and previously accomplished risk assessments:

- Append - Explained briefly in chapter 5.
- Index/sort - Explained briefly in chapter 5.
- Summarize - This method is explained in more details in chapter 5.4. It is also one of methods forming CAISAM and its use in particular audit process is described in chapter 7.
- Calculated column or field – Explained briefly in chapter 5.
- Duplication detection - More on duplication detection method can be found in 5.6. It is also one of methods forming CAISAM and its use in particular audit process is described in chapter 7.
- Selection (extraction) - Further explanation of this method can be found in 5.2. It is also one of methods forming CAISAM and its use in particular audit process is described in chapter 7.
- Gaps - Explained briefly in chapter 5.
- Join - This method is explained in more details in 5.3 and used in CAISAM as presented in chapter 7.
- Stratification – A method is explained in more details in chapter 5.5 and used in methodology explained in chapter 7.

- Benford's Law – Benford's Law is and is explained extensively in chapter 6 and represents the basis of the computer assisted information systems auditing methodology designed and verified in chapter 7.
- Rounded values - More detailed explanation is presented in chapter 5.7. It is one of methods included in CAISAM designed and verified in chapter 7.
- Horizontal analysis - It is explained briefly in chapter 5.
- Vertical analysis – Method is explained briefly in chapter 5.
- Trend analysis - Explained briefly in chapter 5.
- Correlation – Explained briefly in chapter 5.
- Regression – Explained briefly in chapter 5.
- Pivoting – Explained briefly in chapter 5.
- Sampling – Explained briefly in chapter 5.

Appropriate CAAT should include all of abovementioned methods. However, the final decision which methods will be used in specific audit should be dependent on the chosen methodology. That means usually just a portion of outlined methods will be used in any concrete audit. For example, if CAISAM developed in chapter 7 is used, only Benford's Law, selection, join, summarization, stratification, duplication and rounded values methods would be applied. So, conclusion is that CAAT must be flexible enough to enable use of various sets of methods within different methodologies.

Generally speaking, CAATs may be used in performing various audit procedures, including the following [38]:

- identification of transactions that undermine predefined business rules,
- transactions accuracy testing through recalculations,
- testing of accounting entries and balances in the accounting system
- identification of data inconsistencies and significant oscillations,
- execution of sampling methods for audit,
- compliance tests of general computer controls, e.g. comparing the configuration of the operating system, database, firewalls or other IT component recorded in documentation to actual situation,
- testing the correctness of a programmed control,

- checking of inappropriate or unauthorized use of applications and IT equipment

More specifically, CAATs may be very efficiently used to test against risks associated with purchase, sales, inventory, accounting or financial functions. Examples of such tests that can be performed by CAATs are:

- Purchase of goods for which current stock level is greater than established and accepted maximum
- Purchase of goods that have turnover rates lower than defined and accepted
- Purchase of goods with stock level already satisfying long period of needs
- Analysis of automatic re-order procedures (relating to time and stock level) – some may be based on the past activities which are not valid anymore
- Analysis of re-order procedure for low turnover goods
- Comparison of purchase price and storage costs with selling price
- Analysis of contract price breaks and actual purchasing in order to find uneconomic purchasing
- Sales to or purchases from entities with whom employee is somehow related
- Sales in month before the end of an accounting period with terms more favourable than previous months in order to get larger bonuses
- Analysis of order cancellations by salesmen after the end of an accounting period
- Sales not matching to terms set in customer contracts
- Unusual entries to the accounts receivable
- Differences between sales or purchase journals and the general ledger
- Check of goods with exceeded shelf-life levels
- Comparison of inventory turnovers for specific goods in a few past periods
- Unacceptably slow inventory turnover
- Analysis of decreases in inventory balances without corresponding increases in sales
- Check of goods with high write off rates
- Analysis of turnover rates by goods in different locations, if applicable
- Check of goods with unusual changes in percentage differences between purchase and sales prices
- Increases in certain goods in inventory previously not analysed by the auditors

- Check if purchase quantities are based on the quantity required to fill orders, not on quantity price breaks set in contracts
- Analysis of amounts of invoices which is just below the threshold level for review and approval by management
- Search for invoices received from companies with the same address and/or phone number as employees
- Search for companies with different names and same corresponding address and phone number

All of abovementioned tests should be based on predefined (built-in) data manipulation functions. Creation of specific tests should be enabled through query by example interface which does not force auditor to program specific functions since programming is usually cumbersome and complex, while auditors are usually not trained for such tasks. CAAT must enable use of predefined and intuitive interface towards audit methods allowing auditor to focus on his/her primary objective which is audit process and not on computer tools and/or programming.

There are other useful characteristics apart from methods for data analysis that should be supported by CAAT in audit execution phase. One of mandatory properties of efficient tool is export function. Export function enables the auditor to create a new file filled with data from selected data table. It is welcomed if CAAT ensures different exporting formats like Microsoft Excel, ASCII delimited and/or fixed width column files, RTF, XML, HTML, dBASE, Lotus etc. With exporting function it is possible to share data with other auditors (e.g. internal audit, state officials and institutions), who does not need to use the same CAAT software, or to present results to auditee.

CAAT should incorporate adequate script or programming language for additional automation of customized auditing functions invented and designed by the auditor. It is the fact that auditing tasks and use of methods are differing substantially. That fact will never be changed and commercially developed CAATs will probably never include every imaginable function or method. Also, since computer assisted auditing methodologies are not developed and widely accepted, auditors still have different needs for automation of existing methods which are included in CAAT. However, it is necessary that adequate change management and development procedures are managed properly and that

cooperation is established between auditing team and information technology personnel. Auditing team should specify, design and test additionally programmed auditing methods, while information technology personnel should execute programming task.

Macro recording option should be enabled. That option ensures generation of program code based on scripting or programming language. Generated program code, called simply macro, may be used for automation of audit function. Macro recording should be enabled on the level of so called point&click, which means that auditor generates a macro by mouse clicking certain menu choices, button and data contained within CAAT. Generated code must be based on scripting or programming language otherwise supported by CAAT. That way, auditor or an IT programmer may inflict changes in generated code in order to additionally customize its behaviour. By the use of macro recording, certain automated audit function can be implemented quicker and without necessary programming knowledge. So, it may be said macro recording function of CAAT is a natural extension to its script or programming language. A number of audit activities may be automated using macros. Only reasonably advanced functions will not be covered by macro generation but will have to be programmed instead. Of course, auditor must take reasonable care about recorded or programmed macros. It is mandatory to assure documentation, adequate testing procedures and integrity of custom developed macros.

Very useful option that should be included in CAAT is descriptive statistics capability. It provides basic statistical information about all date and numeric columns within any chosen data tables. It should be available and displayed on demand for all records in the data tables without any selection criteria. At a minimum, descriptive statistics for any number column should include following:

- Total value of the column, with positive or negative sign considered (net value)
- Sum of the absolute of the values in the columns (gross value).
- Number of records in data table.
- Number of records with a zero value in the column.
- Number of records with an empty (null) column.
- Sum of debit (positive) values in the column.
- Sum of credit (negative) values in the column.
- Count of records with debit (positive) values in the column.

- Count of records with credit (negative) values in the column.
- Average value of column.
- Minimum value in the column.
- Maximum value in the column.
- Ordinal number of the record that contains the minimum value in the column.
- Ordinal number of the record that contains the maximum value in the column.

For any date column in a data table, descriptive statistics should comprise:

- Number of records with an empty column.
- Number of records in the database.
- Earliest date in the column of a data table.
- Latest date in the column of a data table.
- Ordinal number of the record that contains the earliest date in the column.
- Ordinal number of the record that contains the latest date in the field.
- Number of records for each particular day of the week.
- Number of records for each particular month.
- The day of the week that most frequently appears in the date values in the column.
- The month that most frequently appears in the date values in the column.

Descriptive statistics give a valuable initial analysis of the data table, helping auditor to improve his/her understanding of data and even identify some initial problems that should be furtherly investigated.

During the course of audit process assisted by CAAT, auditor often needs to create mathematical expressions i.e. equations. Equations could be used in various situations: when defining selection equations, creating calculated column, search across all columns etc. Writing such equation expressions without any additional help could be quite complicated and time consuming. Therefore, equation editor is a solution for such situations. It can help with creation of various functions like character, numeric, financial, date and time, matching, conditional etc. The equation editor should assist with entering equations by offering column and table names, functions in their syntactically correct form

and including checking the syntax of entered expressions. Equation editor should enable use of columns, functions, mathematical operators, logical operators, and constants.

Audit work must be based on original and correct data. The integrity of the data should not be jeopardized even during the audit process. That is the reason why CAAT must prevent data from being modified after they are already stored in the tool. Of course, formatting and generation of new data which are the outcome of audit process must be allowed (like results of selection process, calculated columns or fields, summarization totals etc.), but these changes should not affect the integrity of original data imported from production databases.

Visualization may be of additional help during the audit process. Effective CAAT should include the capability to generate diagram charts based on the original data or on data resulting from audit methods application. Diagrams are used to display series of numeric data in a graphical format to make it easier to understand large quantities of data and the relationship between different series of data. Diagrams based on both two-dimensional and three-dimensional views are desirable. Also, at least few diagram styles are required (column, curve, pie). This option is also very useful in reporting phase of audit process when the results of audit are presented to customer (auditee), auditor's management or legal institutions.

In the course of time, auditor is engaged in a number of different audit processes. All documentation should be preserved and separately stored for each audit. The same situation applies when CAAT is used during the audit. That means CAAT itself must enable separation of data and audit results for each individual audit process. This must be implemented on a logical level of the CAAT, so that data from different audits are stored within separate working area. Working areas may be based on database structure or on file structure on the operating system level. It is mandatory request that working areas can not unintentionally interfere with each other, so that data can not be accidentally mixed. A way for easy identification of each working area must be ensured within CAAT. It may be done by assigning properties of each audit such as name of company being audited, name of auditor, time period of audit conduct, business function being audited etc.

One of very efficient properties that should be supported by CAAT is so called search capability. Search capability looks for certain string (text, number or date) within whole

data table independently of columns. So, auditor needs to define string which will be looked for and the data table across which the search will be performed. Search is always executed across all columns and records in data table and it may or may not generate new data table. It is very useful as a mean of quick scan for certain data without previously guessing in which column data of interest could reside.

Very useful and already default capability of any modern software product is so called "copy&paste" attribute. Copy&paste enables copying of selected values in columns and/or records and pasting them in another, or target, location. In CAAT, pasting is allowed only if it will not change the data in tables. So, pasting should be allowed only in equations and expressions as well when the need for pasting to different software tools is needed. For example, it may be useful to copy data from result of audit method and paste it in Microsoft Excel or Word.

Since some data tables may have a fairly large number of columns, it is very practical to have an option for certain columns freeze. When certain columns are frozen, auditor will always see those columns while scrolling across the remaining columns is also enabled. It makes much easier insight in all columns and comparison of frozen and scrolled columns across records. Also, for the same reason of better data inspection, it is desirable that auditor may hide certain data table columns. This option temporarily hides chosen columns from the CAAT board and enables focus of auditor to remaining columns.

Efficient situation sensitive help system within CAAT is necessary. It must offer help topics according to position in menus or methods being used. Help system must cover at least following topics:

- what is the specific CAAT and its basic capabilities
- how the use of CAAT should be planned and controlled
- what audit methods are included and how they may be used
- how CAAT can be navigated (explanation of menus, windows and toolbars)

Especially important component of help system is the one that explains what real life business activities may be audited and how. Also, web based help desk for reporting of issues, bugs and questions concerning usage of CAAT is indispensable.

8.1.3 Audit Documenting

The complete audit process supported by CAAT must be adequately documented. Only documented audit process makes sense, because basic and mandatory prerequisite is to ensure valuable audit results. The audit documentation must include extensive description of CAAT implementation during the whole audit process (planning and execution).

Documentation in the planning audit phase must define:

- Objectives of CAAT application and business function and processes that will be covered
- What CAAT will be used
- What CAAT methodology will be applied
- What experts on auditor and auditee side are necessary
- Time and other resources

Documentation in execution phase should include:

- Process of data acquisition and eventual preparation for audit
- Description of data acquired
- Step by step description of audit execution according to applied methodology

Documentation must include all steps performed within execution phase including the creation or deletion of data tables, as well as each method execution. All changes must be saved in the detailed audit trail which must be inaccessible for change by the auditor. That way the steps and methods performed may stay intact, authentic and available for further inspection if needed.

Documentation of audit results must comprise of:

- Data outputs from applied audit methods
- Description of the audit work performed on the output of audit methods
- Audit findings
- Audit conclusions
- Audit recommendations

All original and resulting data must be stored in a secure storage. It is mandatory that all audited data is encrypted and keys for encryption stored in accordance with assessed risks.

Furthermore, the same procedure must be followed for temporary classified data used or created in the audit process.

8.1.4 Reporting

The audit report must contain detailed description of planning and execution audit phase. The facts for the report must be sourced from documentation phase which should assure all information from planning and execution. So, it is obvious that reporting phase largely depends on quality of documentation generated during planning and execution phase of the audit conduct. The audit report must contain clear definition of objectives, scope and CAAT methodology. Methods used in methodology must be briefly introduced and CAAT that was used must be described.

All deviations from the audit plan must be described and explained. All input data, their relation to business function and processes must be described. Results of CAAT use must be commented. Special attention must be given to errors, omissions or frauds.

CAAT must have important role in reporting phase. It must cover the printing of results in adequate report format. Also, CAAT must include export of generated reports in widely accepted formats (Excel, Rich Text Format, Word, Extensible Markup Language, HyperText Markup Language, or Portable Document Format). Adequate integration with existing de facto standard word processors is indispensable.

8.2 Improvement of Auditor's Work Quality

A number of benefits of CAATs use are already noted in previous chapters. However, CAATs advantages that can improve auditor's quality of work will be briefly described.

As companies and institutions use information systems to store and process constantly increasing amounts of data, the necessity grows for definition and use of auditing procedures in producing adequate risk assessment concerning data management. CAATs are becoming increasingly important tool in evaluation of the control mechanisms in more efficient course. Application of CAATs improves audit scope, completeness and consistency of data analysis. This all together leads to more effective operational and information systems risk mitigation.

With CAAT it is much easier to implement strict auditing methodology. It is possible to define strict steps and use of specific methods in order to perform comparable and standardized audits. That way, it is possible to compare audits along longer timeline and to employ early warning system through continuous data audits. Continuous data monitoring is an ongoing process for data provisioning, analysis and reporting in order to identify and react to operational risks. To assure comprehensive approach for provisioning, analysis and reporting, auditors should give the recommendations how continuously monitoring of user activity on all computer systems supporting business transactions and applications. With such system, efficiency of an auditor using CAAT in discovering fraud, omissions and errors would drastically improve.

CAATs ensure auditor's work is flexible and innovative as well as providing improved audit performance. The application of CAATs during the audit execution phase can also help auditors to adjust and improve their initial methodology in response to audit results. Of course, changes in methodology must be controlled and under strict change management process. CAATs enable auditors to more focus on audit work and reasoning than to lose their time and resources on manual audit steps. Also, result of CAAT use can often lead to unexpected findings in audit data sets.

As it is illustrated in [3] use of CAATs improve data analysis, increase audit scope, assure better use of audit resources, more precise and valuable results.

As data volumes constantly grow and at the same time management expectations on adequacy of auditing process rise, random manual verifications and testing do not produce the desired value. The use of CAAT assures complete coverage of transactions in the audit focus and identification of erroneous or exceptional transactions, even when data volumes are huge. Data analysis tasks like selection, Benford's Law tests, sorting, joining, summarization or stratification may be performed in extremely small amount of time comparing to manual techniques.

CAATs can provide audit organizations with the ability to perform audits which were not feasible before. Business systems that contained tens of millions transaction records are difficult to audit using manual techniques. So, together with today's enormous computing power of personal computers, CAATs may analyze millions of transactions in matter of minutes.

CAATs enable conduct of audit process off-site. That means, after data is provisioned and stored on personal computer, auditor may audit the data out of client's premises. So, travel costs may be significantly reduced as well as the time needed for audit execution. This advantage of CAATs is even more emphasized if data must be collected from large number of different locations. If auditor would have to travel to and perform complete audit on each location, expenses and time needed for audit conduct would grow significantly.

Knowledge and abilities of auditors is considerably rising as a consequence of use of CAATs. If auditors must perform a numerous manual and thus non-productive procedures, they will have little time left to focus on important data issues. CAATs may free auditors from routine, simple, repetitive but time consuming tasks. They will allow auditor to spend more times on activities requiring the application of auditor's judgement and reasoning. Forcing the computer to handle repetitive tasks, calculations, selections and other auditing methods the auditor's resources and focus on audit may be maximized. As auditor's work is usually expensive, this means auditor may perform more tasks in less time thus reaching better cost effectiveness levels. Additionally, freeing auditor from repetitive and routine tasks usually improves job satisfaction.

Conduct of thorough analysis of entire audit data set in significantly shorter time is enabled by CAATs. CAATs provide numerous specialized auditing methods which can be applied on huge volumes of data in a fraction of time.

CAATs also provide log or audit trails which allow easy review of audit results for accuracy. Such log files may also serve as a proof that certain methods and steps were executed during the audit conduct. That can be of a major importance when auditor's findings differ from management opinion which is declared through management comment letter.

CAATs can positively influence on development of audit reports with statements of significance and materiality. Report will be more focused on audited business function, complete, accurate, better supported by the audit evidence, finished on time and easier to understand to management of auditee since it is based on their business data. Those improved characteristics may contribute to the acceptance of the audit findings and recommendations. Also, auditee's opinion on capabilities of an audit organization may be significantly elevated. Also, results of audit in form of reports may be stored and organized

within auditor's knowledge base which can be accessed by other auditors according to access rights and sensitivity of information. That can serve as basis for improvement of auditors' knowledge on computer assisted audit methodology and business function being audited. Furtherly, since CAATs generate adequate audit trails and thus enhance audit documentation during audit execution phase, reporting phase may be less time consuming, more informative and understandable. Information gathered through CAATs can amend the planning, execution, documentation and reporting phase of other audits. Also, it must be used in eventual follow up audits.

Audit conducts are usually organized as projects, with assigned project leaders, time, personnel, money, hardware and software resources. Project management is usually very demanding, since usually more projects are executed at the same time, and unfortunately, the same experts and other resources are often assigned to more than one project. Fortunately, CAATs may be used to support audit projects. More precisely, project leader can easier review ongoing results and give each team guideline or advice when needed if audits are performed with CAATs. The ability to extract and analyze data, examine and control auditor's results can provide team leader with assurance that audit work is performed adequately and in alignment with pre defined methodology. Use of CAATs can result in better planning of audits, management of audit resources, better control of alignment with accepted audit methodology, clearer identification of risks and significance of results. The ability of audit organization to execute audits in given timeframe and considerable quality can be amended by effective access and analysis of data with CAATs. The integrity and relevance of audit findings can be made more trustworthy if checked, analyzed and proved by CAATs methods.

Improvement of auditor's work can be indirectly obtained by transfer of audit technology. As it is described in [3, pages 101/2] "once the audit organization has embraced the use of automated tools and techniques, it will be better positioned to have a major impact on the operations of the (client's) organization. This can include the provision of tools and techniques to the clients. Traditionally, whether to ensure independence or for other reasons, many audit organizations have attempted to maintain their distance from the client. More recently, audit sees the client as more of a potential beneficiary of audit's services... Auditors are trying to keep pace with the organization as a whole and are interested in assisting clients in improving their efficiency and effectiveness. This can take

many forms, from the development of self-assessment tools to the transfer of knowledge, tools and techniques." With the transfer of CAATs to client's internal audit department, lot of internal audit functions may be improved. That may further enhance the work of external auditor who will be able to focus on more complex business functions or those functions not covered by internal auditors.

Important feature of CAATs is user friendly interface which enables auditor to perform all audit methods, irrespective of the database structure or corresponding information technology which is basis for information system. Such interface uses much of standard windows properties so learning curve may be extremely steep and short.

To conclude, basic benefits of CAATs include:

1. Possibility to use consistent and standard computer assisted auditing methodology.
2. Many audit-specific methods are included, thus analytical capabilities are enormously increased.
3. Improvement of auditors' knowledge about the audited area.
4. Auditors are more focused on judgement, reasoning and thinking.
5. Improved integration of business system and information system audit.
6. Better environment to improve audit methodology.
7. Increased cost-effectiveness because of reusability and customization of methods.
8. Independency of the system being audited by use of read-only copy of the file to avoid any corruption of an organization's data.
9. Complete coverage of data sets avoiding errors in data sampling.
10. Provision of documentation of each test performed in the software that can be used as documentation in the auditor's work papers.
11. Improved reporting capabilities.
12. Possibility of off-site audit conduct.
13. Improvement of management of audit organization.
14. Standard interface assures quick learning process.

It may be concluded that this chapter contains some most important advantages of CAATs which can distinctively improve the quality of auditor's work. Of course, there are numerous additional features that some auditors may find very useful which are not included here.

8.3 The Challenges in Implementation of Computer Assisted Auditing Tools

Although it is explained that CAATs are extremely useful software tool, there are also numerous challenges that should be understood. These challenges must be treated adequately in order to prevent problems and even cancellation of CAATs use within audit organization.

It is very important that auditors get and improve sufficient knowledge on CAAT, its capabilities, possible ways of use in audit process as well as risks in CAAT use. Auditors also must have certain knowledge of information technology, especially some basics of relational theory. That is mandatory since data records are stored in data tables, uniquely identified by primary keys and related to each other by foreign keys. Understanding of data and business (chapter 8.1.1), relating data to business processes and events is of crucial importance to successful use and implementation of CAATs.

Definition and acceptance of computer assisted auditing methodology is one of major prerequisites in reaching the adequate level of CAAT use. It is not sufficient if auditor only understands the technical and analytical capabilities of CAAT. What is of even bigger importance is necessity to understand, accept and use appropriate methodology. Only then, auditing work within certain audit organization may be standardized, comparable and repeatable. Also, use of methodology has the advantage of permanent improvement of audit process since auditors may comment and suggest changes in steps, methods and their relationships. Of course, process of methodology change management should be established with objective to adequately control modifications.

Although acceptance of computer assisted auditing methodology is indispensable, auditors should also identify additional CAAT opportunities. That means auditors should actively seek for business areas in which CAAT were still not used and assess usefulness of CAAT application. It may be useful if auditors within audit organization develop guidance which explains different applications and specifies examples of the information that can be gained from each application. Some lessons learned could be listed including successes and failures. These lessons can be used to help audit organization continue to learn and improve the use of CAATs. Monthly summaries which briefly outline the use of CAATs in each current audit can help auditors realize additional opportunities for the CAATs use. [3,

page 168]. That could result in additional quality of audit work since more business areas would be included in audit process. Also, that will help an audit organization to widen its scope of audit and to gain more market share. Identification of additional CAAT opportunities should be associated to change management of computer assisted auditing methodology.

Management must be devoted to the use of CAATs and has to actively promote their use and development of methodologies that are basis of CAATs. Management support should not cease with promotion and formal commitment, but with assurance of enough resources needed for adequate education and use of CAAT. As it is noted in [3, page 170] the implementation of CAATs in the audit environment will probably involve change in ordinary audit processes and procedures. Usually, audit resources (experts, time, knowledge) are already close to the limits and quite restrained concerning new initiatives and ideas. If audit organization works on a fee from external customers then the question who will bear the development and implementation cost of a new idea is usually very important. In order to ease these problems, audit management should find so called "champions of idea". Champions of idea are auditors who accepted the idea of CAATs and are willing to implement it in audit environment. Some other important issues that must be ensured and resolved by management are:

- money for education and CAAT software purchase and maintenance
- time for education
- permanent use and update of adequate methodology
- resistance to change by some auditors
- relieving auditors using CAAT from other audit duties

Some auditors will very quickly adopt and understand most of the CAAT capabilities and methods, while others will require support and help. Also, each auditor or audit team will surely need help within some auditing steps (planning, execution, documentation and reporting). Technical and analytical support and advice is of major importance when using CAAT. Auditors using CAATs should not be let on their own, but supported by knowledge of other auditors, specialized CAAT help desk and/or support provided by vendor of CAAT.

Although CAATs are very powerful software tools, expectations of audit management may not be met. As described in [3, pages 170/1] even when the effort to use CAAT in audit

automation is perceived as innovative and advanced, management's expectations may be unreachable or completely different. Auditor should bear in mind that lot of projects fail because they did not meet the expectations which were too optimistic and probably unattainable. So, well defined deliverables and timeframes should be established and accepted. It must be agreed what resources (personnel, time, hardware, software) will be assigned to CAAT implementation project. As automation of audit function by use of CAAT is usually not a primary task of those resources, it must be clearly determined what priority will be given in comparison to other tasks. Management's expectations must be answered by clear and understandable statements. Special attention must be given to cost-benefit analysis which is usually crucial factor in management's decision of whether or not to start CAAT implementation. So, in order to minimise the risk of CAAT implementation failure their use must be linked to the objectives of the audit organization.

Although some audit organizations were determined in introduction of CAAT in their audit environment which resulted in appropriate implementation, certain auditees did not welcome the idea. This misunderstanding is more often if there is no legal act which binds auditees and auditor on usage of CAATs. Anyways, auditor should inform client that more value will be gained from audit process if CAAT is used. Crucial issue is to appropriately explain cost and benefits of CAATs use in order to establish client's clear expectations. There is also a necessity to communicate and agree on access to production database to client's information technology department. Some misunderstandings are possible, so auditor must clearly state what are audit needs and how and what data should be extracted. More on the issue of data provision may be found in chapter 8.1.1.

A number of audit clients are reluctant to export production data to auditor's computers. The principal reason is concern that data will not be managed appropriately i.e. lost, accessed by unauthorized persons within or out of auditor organization or inappropriately manipulated. Auditor must define clear procedures on client's data management and storage especially concerning confidentiality of data. Client's data should be encrypted and all computers storing data must be protected by authentication procedure on operating system and database level. These procedures must be communicated to client. Although clients are legally obliged to present all data to auditors, and auditors are legally bound to appropriate data management and data secrecy, some form of personally signed non disclosure agreement between each individual auditor and client could be arranged.

The only contact between client's management and CAAT is during the presentation of auditor's findings and recommendations. In order to show auditing was valuable for client and to adequately promote the use of CAAT, presentation must concentrate on relevant findings and recommendations. Auditor must spend considerable time in relating data analysis findings to business activities and to prepare presentation of data analysis findings in the way management sees data. It is quite important since client's management usually does not have relational view of data in mind. Presentation of recommendations can be especially demanding and auditor must find the appropriate way to present what measures must be undertaken to avoid eventually recovered errors, omissions or frauds.

Use of CAATs must prove itself among auditors and business entities being audited as a useful software tool. If CAAT is not used adequately, as presented in chapters 8.1.1 to 8.1.4, and if it does not prove its usefulness, then the results will not justify efforts made to apply CAAT. The outcome could be that both auditors and auditees will start to deny adequacy of CAATs. Such situation will inevitably lead to abandoning CAAT or, if its usage is required by legal acts, using it just to fulfil formal obligation. That will of course result in even less appropriate use and less useful audit findings.

Sometimes auditors develop CAAT on their own believing they can build a software tool which is more appropriate and more specialized for use in their audit processes. However, the advantages of computer assisted auditing tools and their built-in functions in comparison to self developed programs and functions by the auditors themselves are numerous:

- auditors focus on audit instead on spending time and resources on development of programs and functions
- burden of program and functions development is transferred to specialized company
- accuracy, quality and choice of functions is in favour of commercial product because commercial companies which develop software usually have specialized staff and adequate advanced expertise in software development
- commercial companies usually have broader knowledge on different audit cases and possible use of computer assisted auditing tools

It is very important that auditors do not spend their time and effort in development of CAATs since on the market there is considerable number of commercial CAATs with fairly advanced capabilities.

It may be concluded that challenges explained in this chapter are not the only auditing organization could encounter in implementation of CAAT in audit environment. However, following directives outlined in this chapter should help in avoidance or mitigation of majority of risks and problems that inevitably appear during the CAAT implementation.

9. Achieved Objectives and Confirmation of Hypotheses

In this chapter, achievement of objectives and confirmation of hypotheses set in chapter 1.2 will be discussed.

In many institutions and business entities, data are the most valuable assets which are very often identified as extremely important means on which management bases its decisions. Also, in chapter 2 few examples based on improper data manipulation that ended with enormous financial losses and even bankruptcies are presented. It was shown that all of these cases could have been prevented if data were appropriately audited. Of course, manual execution of audit was out of question since data quantities were extremely large. Only possibility is to perform computer assisted auditing i.e. audit of data stored in databases with the help of specialized software tools consisting of various data auditing methods. Thus, needs for application of computer assisted information systems auditing are identified.

Approaches, frameworks and methods for information systems audit were introduced by Information Systems Auditing and Control Association, Bank for International Settlements, International Monetary Fund, central banks, auditing authorities and legal acts. Some frameworks and approaches were explained and evaluated in chapter 4. A number of methods for computer assisted auditing were presented in chapter 5. Evaluation ended with conclusion that adequate methodology for computer assisted auditing does not exist. More details on achieving objective of identification, systematization and evaluation of existing approaches, frameworks and methods for computer assisted auditing can be found in chapters 4 and 5.

In chapter 6, various Benford's Law tests are explained in details: the first, the second, the first two and the first three digits tests are encompassed. Benford's Law proved to be very powerful method for computer assisted auditing. One of its principal strength is the fact that auditor does not have to define in advance what type of fraud, error or omission should be investigated. Only after the specific test is executed, auditor should question results and compare eventual deviations with previously set business norms, data creation and modification rules. More on conclusion that Benford's Law may be used as backbone

method within computer assisted information system auditing methodology is noted in chapter 5.

Methods that form computer assisted information systems auditing methodology (Benford's Law, selection, join, summarization, stratification, duplication, rounded values) are defined and adequate conclusion is brought up in chapter 5. Benford's Law, as the fundamental method of developed CAISAM, is very extensively explained in chapter 6.

Meta-model of CAISAM is designed in chapter 7.1. That meta-model represents a model suitable and applicable to any particular CAISAM. After meta-model is designed, model of particular computer assisted auditing methodology is created and explained in details in chapter 7.2.

Sequence and relations between specific methods are defined in chapter 7.2. Developed CAISAM is defined with 15 steps in which particular methods are applied on data. In some steps more than one method is used. After data provision step, supported by selection and join methods, audit sample check must be done by use of selection, summarization, stratification and join methods. All four Benford's Law tests explained in chapter 6 are to be executed on complete audit sample – if certain subset is created and Benford's Law subsequently executed, findings may be erroneous. Checks if audit sample proves fraud, omission or error are supported by selection, summarization, duplication and rounded values methods. Final conclusion on fraud, omissions or errors is also based on selection, summarization, duplication and rounded values methods.

All audit phases including audit planning, execution, documenting and reporting are covered by recommendations for extending of CAAT's functionality. Very valuable instructions for improvement of audit execution phase are given in chapter 8.1.2 like use of descriptive statistics function, methods that should be included in CAAT, export function, scripting or programming language, macro recording function, equation editor, read only data sets, visualization options, search capability, differentiation between audit activities etc. Recommendations for audit documenting are given in chapter 8.1.3. CAATs must perform automatic logging of all important audit activities. Reporting phase must rely on documentation generated automatically by execution of certain CAAT methods and on guidelines set in the audit planning phase.

Developed CAISAM is applied on cross-border payments system data and thus verified. Used audit sample contained of 1.745.311 payment transactions. Certain deviations were detected and explained with significant help of designed CAISAM. Additionally, with CAISAM audit process becomes repeatable, comparable, consistent and executed faster with less auditing resources.

There are two hypotheses set in chapter 1.2:

H1: It is possible to develop CAISAM
Hypothesis is proved in chapters 7.1 and 7.2 since meta-model and model of particular computer assisted information systems auditing methodology are defined. Instructions for use of methods within defined methodology are presented. Sequences and relations between methods that form CAISAM are demonstrated and explained in details.

H2: Auditing process may be improved if developed CAISAM is applied
CAISAM is applied on cross-border payments system data (chapter 7.3.3). It is clear that without CAAT auditing of 1.745.311 data rows would not be feasible. Additionally, use of developed CAISAM proved significant improvement in audit process. Certain deviations, that would not be recovered otherwise, were found. Since strict methodology enables execution of repeatable, comparable and consistent audit processes, which are unreachable properties if computer assisted audit is not based on methodology but on improvisation, it proves audit process is significantly improved.

10. Conclusion

Because of increasing data volumes that should be regularly audited, it can be easily concluded that technology must be used in order to make considerable improvement of audit conduct. Today, manual audit of business data is practically impossible task. Even if it is performed, it lacks completeness since it is not feasible to audit all data without technology support. Also, use of manual auditing methods is by definition prone to omissions and errors. So, in order to adequately perform audit work, auditor must use computer based tools.

Of course, in order to find flaws which can result in frauds, omissions or errors, auditor must have extensive knowledge not only about computer technology and application development but, what is even more important in this case, business knowledge and knowledge about data used in certain business environment. Auditor must clearly understand what data is expected on input side, what formal and logical controls should be implemented at the entry i.e. input level and in which form data should be stored in the system. Also, mapping and matching the data in the system with data on some other media i.e. paper forms could also be mandatory. That is necessary in systems which are still based on paper documents as means for storing data prior to computer data entry function. Only person who has such knowledge can analyze data and make conclusions about correctness of input controls. Of course, in order to check data processing algorithms, auditor should have detailed knowledge of business logic and how it transforms data (calculations and formatting, for instance). Whether business logic is implemented accordingly, can be concluded by checking application code or by comparison between input and output (result) data. For application code check, auditor must have advanced knowledge of certain programming language, development environments and, of course, certain business function. Anyways, it can be quite cumbersome task since business logic can be supported by very complex application code modules. Reading and analysing underlying program code requires significant time and specialized technical knowledge. In practice, comparison between input and output data is more usual way of business (application) logic audit. When using such approach, it is not necessary to check through application code. Business logic part of application is considered black box, and concentration is set on

creation of input data set and evaluation of resulting output data. If output data is correct, one can conclude application logic is correct. This approach requires more knowledge about data and its transformation from input to output, but less or none knowledge about underlying programming languages and development environments. Some specialized computer based tools can be of enormous help to this approach. A family of extremely practical tools are computer assisted auditing tools (CAATs). CAATs have numerous benefits over manual techniques, especially in following:

- achieving complete data check even on large databases
- providing many pre-defined audit specific methods
- ensuring methods standardization
- ensuring independency from the audited information system by various data access methods
- using only read-only copy of business data
- enabling import to personal computers, thus avoiding performance degradation of targeted computer system
- assuring documentation of each applied method or step of methodology

However, supporting technology in audit work already exist for years. Anyways, audits are still inappropriate i.e. incomplete and often without added values. Also, such audits can encourage fraudulent activities, errors and negligence. Although prominent organizations for audit improvement (ISACA) as well as state authorities (e.g. FED, CNB) promote and force specific audit frameworks and approaches, still numerous problems exist. Previously mentioned regulations together with frameworks and approaches give an overview and specific highlights how audit should be executed. Their primary fault is lack of details, thus increasing possibility of various understanding and interpretations. Furtherly, although data auditing is indispensable component of each auditing process and use of CAATs is promoted and forced by use of authorities, still there is no accepted computer assisted auditing methodology. Without strictly established methodology each audit is commenced with different methods, their order and mutual relationships so conclusions on errors, omissions or frauds are based on different premises. One of outcomes of such situation is that two data audits of same data and business subject are usually not comparable and have different conclusions. Data auditing methodology is indispensable for improvement of audit process and adequate use of computer assisted auditing tools.

In this thesis it was proved it is possible to develop computer assisted information systems auditing methodology (CAISAM). CAISAM was developed on the basis of Benford's Law and six other supporting methods: selection, join, summarization, stratification, duplication and rounded values.

Second hypothesis, that auditing process may be improved if developed CAISAM is applied is proved in practical auditing of cross-border payment system. During that audit it was shown that CAISAM is very useful and that it significantly improves auditing process.

11. References

[1] Bandler J., Varchaver N.: "How Bernie Did It", CNNMoney.com, http://money.cnn.com/2009/04/24/news/newsmakers/madoff.fortune/index.htm?postversion=2009042412, accessed 24th of June 2009.

[2] Brooks, D.: "War, Politics & Customer Loyalty: forecasting Using Benford's Law", Frequencies – The Journal of Size Law Applications, Ekaros Analytical Inc., Vol 1 no 1, 2001.

[3] Coderre D.: "CAATTs and Other BEASTs for Auditors", Global Audit Publications, Vancouver, Canada, 2001.

[4] Coderre D.: "Fraud Detection – A Revealing Look at Fraud", Ekaros Analytical Inc., Vancouver, Canada, 2003.

[5] Dragičević, D.: "Kompjutorski kriminalitet i informacijski sustavi", Informator, Zagreb, 1999.

[6] Durtschi C., Hillison W., Pacini C.: The Effective Use of Benford's Law to Assist in Detecting Fraud in Accounting Data, Journal of Forensic Accounting 1524-5586/Vol. V, 2004., pages 17-34

[7] Hill, T.: "A Note on Distributions of True Versus Fabricated Data", Georgia Institute of Technology, Atlanta, www.git.edu, accessed 25th of August2005.

[8] Hill, T.: The First Digital Phenomenon, American Scientist, v86 n4, 1998., pages 1-6

[9] Hill, T.: "The Significant-Digit Phenomenon", Georgia Institute of Technology, Atlanta, www.git.edu, accessed 25th of August 2005.

[10] Krakar Z., Žgela M.: "Application of Benford's Law in Payment Systems Auditing", JIOS Journal of Information and Organisational Sciences, Vol. 3 No. 1, 2009., pages 39-51

[11] Krakar Z., Žgela M.: "Evaluation of Benford's Law application in stock prices and stock turnover", Society and Technology 2008, Zadar, Croatia.

[12] Lanza R.: "How to Use a New Computer Audit Fraud Prevention and Detection Tool", Information Systems Control Journal, Vol 1, 2004

[13] Lanza R.: "Proactively Detecting Occupational Fraud Using Computer Audit Reports", The IIA Research Foundation, Altamonte Springs, USA, 2003.

[14] Matthews R.: "The Power of One", http://members.fortunecity.com/templarser/one.html, accessed 13th of August 2009.

[15] Milton A.: "What are Futures", http://daytrading.about.com/od/futures/a/

WhatAreFutures.htm, accessed 15th of May 2009.

[16] Nigrini M.: “Benford’s Law”, http://www.rexswain.com/benford.html, accessed 28th of June 2008.

[17] Nigrini M.: “Digital Analysis Using Benford's Law”, Global Audit Publications, Vancouver, Canada, 2000.

[18] Nigrini M.: "I've Got Your Number", Journal of Accountancy, Vol. 187. Issue 5, 1999, pages 79-84

[19] Nigrini M., Mittermaier L.: “The Use of Benford's Law as an Aid in Analytical Procedures”, Auditing - A Journal of Practice & Theory, Vol. 16, No 2, 1997., pages 52-67.

[20] Opaska W.: "Survey of Accounts Payable Disbursements", available at http://www.fcc.gov/Bureaus/Inspector_General/Reports/surveymemo.txt, Accessed: 27th March 2008.

[21] Posch, P.: "Benford or Not Benford? How to test for the First-Digit-Law", University of Ulm, Working Paper, 2004.

[22] Posch, P.: "A Survey on Sequences and Distribution Functions Satisfying the First-Digit-Law", University of Ulm, Working Paper, 2004

[23] Sayana A.: “The IS Audit Process”, Information Systems Control Journal, Volume 1, Rolling Meadows, USA, 2002.

[24] Sayana A.: “Using CAATs to Support IS Audit”, Information Systems Control Journal, Volume 1, Rolling Meadows, USA, 2003.

[25] Schneier, B.: "Beyond Fear: Thinking Sensibly About Security in an Uncertain World", Copernicus Books, New York, 2003.

[26] Schneier, B.: "Secrets & Lies: Digital Security in a Networked World", John Wiley & Sons, Inc., New York, 2000.

[27] Shinder, D. L.: "Scene of the Cybercrime: Computer Forensics Handbook", Syngress Publishing, Inc., Rockland, 2002.

[28] Silverstone H., Davia H.: "Fraud 101 – Techniques and Strategies for Detection", John Wiley & Sons, Hoboken, 2005.

[29] Singleton, T., Singleton, A., Bologna, G., Lindquist, R.: "Fraud Auditing and Forensic Accounting", John Wiley & Sons, Hoboken, New Jersey, 2006.

[30] Sirikulvadhana S.: “Data Mining As A Financial Auditing Tool”, M. Sc. Thesis in Accounting, Swedish School of Economics and Business Administration, 2002.

[31] Tudor, J.: "Information Security Architecture: an Integrated Approach to Security in the Organization", CRC Press, Boca Raton, 2000.

[32] Turnbull C.: Fraud Investigation Using IDEA, Ekaros Analytical Inc., Vancouver, Canada, 2003.

[33] Viscusi G., Chassany A.: "Societe Generale Reports EU4.9 Billion Trading Loss", http://www.bloomberg.com/apps/news?pid=20601087&sid=a8GBEB7UuuXc, accessed 12th of December 2008.

[34] Wells J.: Corporate Fraud Handbook – Prevention and Detection, John Wiley & Sons, Hoboken, USA, 2007.

[35] Westerman, G., Hunter, R.: "IT Risk", George Westerman and Gartner, Boston, 2007.

[36] Žgela, M., Krakar, Z.: "Design of Framework for Computer Assisted Information Systems Auditing Methodology (CAISAM)", 20th Central European Conference on Information and Intelligent Systems – CECIS2009 Conference Proceedings, Faculty of Organisation and Informatics, Varaždin, 2009., pages 155-165.

[37] ... "About BIS", http://www.bis.org/about/index.htm, BIS, accessed 16th of May 2008.

[38] ... "Audit - IT Examination Handbook", Federal Financial Institutions Examination Council, FED, USA, 2003.

[39] ... "Benford' Law", http://mathworld.wolfram.com/BenfordsLaw.html, accessed 10th of May 2008.

[40] ... "The COBIT Framework Executive Summary", http://www.counterpoint.co.za/ pages/cobit.htm, accessed 20th of October 2008.

[41] ... "COBIT 3rd Edition – Implementation Tool Set", COBIT Steering Committee and IT Governance Institute, Rolling Meadows, USA, 2000.

[42] ... "COBIT 4.1", IT Governance Institute, Rolling Meadows, USA, 2007.

[43] ... "Core Principles for Effective Banking Supervision", Bank for International Settlements, Basel, Switzerland, 2006.

[44] ... "Decision on Adequate Information System Management", Croatian National Bank, Governor's Decision, Zagreb, Croatia, 2007.

[45] ... "G3 – Use of Computer-Assisted Audit Techniques (CAATs)", ISACA, Rolling Meadows, USA, 2008.

[46] ... "International Convergence of Capital Measurement and Capital Standards", Bank for International Settlements, Basel, Switzerland, 2004.

[47] ... "ISACA Overview and History", http://www.isaca.org/Content/NavigationMenu/

About_ISACA/Overview_and_History/Overview_and_History.htm, ISACA, accessed 25th of June 2008.
[48] ... “IS Standards, Guidelines and Procedures for Auditing and Control Professionals”, Information Systems Audit and Control Association, Rolling Meadows, USA, 2009.
[49] ... ”Izvješće o rekonstrukciji poslovnih događaja u Direkciji deviznih sredstava Riječke banke d.d. u razdoblju od 1997. do 15. ožujka 2002.”, Hrvatska narodna banka, Zagreb, Croatia, 2003.
[50] ... "Management - IT Examination Handbook", Federal Financial Institutions Examination Council, FED, USA, 2004.
[51] ... "Operational Risk", Federal Reserve Bank of Chicago, http://www.chicagofed.org/banking_information/operational_risk.cfm, accessed 20th of February 2009.
[52] ... "Report to the Boards of Directors of Allied Irish Banks, p.l.c., Allfirst Financial Inc., and Allfirst Bank Concerning Currency Trading Losses", Promontory Financial Group and Wachtell, Lipton, Rosen & Katz, 2002.
[53] ... "Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika", Hrvatska narodna banka, Zagreb, Hrvatska, 2006.
[54] ... “Sound Practices for the Management and Supervision of Operational Risk”, Bank for International Settlements, Basel, Switzerland, 2003.
[55] … "Uputa o provedbi Odluke o načinu obavljanja platnog prometa s inozemstvom i načinu dostavljanja podataka o platnom prometu s inozemstvom", Hrvatska narodna banka, Zagreb, 1996.
[56] ... "Zakon o bankama", Narodne novine br. 84/2002, Zagreb, Hrvatska, 2002.

DD (FOI)
Tekući broj:
(Sveučilište – Zagreb)

Doktorska disertacija UDK: 004.05 (043.3)

Razvoj metodike za računalno podržanu reviziju informacijskih sustava

M. Žgela
Fakultet organizacije i informatike
Varaždin, Hrvatska

Praksa pokazuje da brojne prijevare zasnovane na računalnoj tehnologiji predstavljaju novi i sofisticirani oblik suvremenog kriminala koji po svojim posljedicama može biti dramatičan, ne samo za pojedine poslovne sustave, već i globalno. Budući da se ovaj oblik kriminala realizira kroz informacijske sustave, njihova revizija, kao sastavni dio potrebnih kontrolnih mehanizama, danas postaje nezaobilazna. No, postojeće metode revizije informacijskih sustava tek se razvijaju i u ovom trenutku još ne postoji njihova metodika. Zbog toga je temeljni cilj ovog rada pokušati razviti računalno podržanu metodiku revizije informacijskih sustava. Polazna osnova za njeno oblikovanje je primjena Benfordovog zakona, kao poveznice postojećih revizijskih metoda. Analiza literature pokazuje da je ovo područje još nedovoljno istraženo. Zbog toga je navedena problematika temeljito obrađena, izrađen je model i razvijena je konkretna metodika za računalno podržanu reviziju informacijskih sustava, načinjen je niz testova i drugih ispitivanja, razvijena metodika je provjerena na reprezentativnom uzorku, te su dani naputci za daljnji razvoj ovog područja i pratećih revizijskih programskih alata.
Područje istraživanja u disertaciji je financijska industrija (sustav deviznog platnog prometa), jer su se u ovom gospodarskom segmentu dogodile najveće pronevjere, koje su i bile moguće upravo zbog nedostatka adekvatnih kontrola, učinkovite i pravovremene revizije informacijskih sustava.

Voditelj rada: Prof. dr. sc. Zdravko Krakar

Povjerenstveno za ocjenu i obranu:
Prof. dr. sc. Josip Brumec
Prof. dr. sc. Ružica Brčić
Prof. dr. sc. Zdravko Krakar
Prof dr. sc. Mario Spremić
Doc. dr. sc. Jasminka Dobša

Datum obrane: **Datum promocije:**

Rad je pohranjen u biblioteci Fakulteta organizacije i informatike u Varaždinu

(204 stranice, 12 slika, 30 tablica, 56 bibliografskih podataka, original na engleskom jeziku)

DD (FOI)

UDK: 004.05 (043.3)

Tekući broj:

I. Razvoj metodike za računalno podržanu reviziju informacijskih sustava
II. Žgela, M.
III. Fakultet organizacije i informatike, Varaždin, Hrvatska

Revizija IS-a
Računalno podržana revizija IS-a
Benfordov zakon
Model metodike
CAAT

DD (FOI)
Current file number:
University of Zagreb
Doctoral Dissertation UDC: 004.05 (043.3)

Development of Methodology for Computer Assisted Information Systems Auditing

M. Žgela
Faculty of Organization and Informatics
Varaždin, Republic of Croatia

A practice shows that numerous frauds based on computer technology represent new and sophisticated form of modern criminal which can cause dramatic consequences, not only for individual business systems but also globally. Since this criminal form is realized through information systems, their audit, as a constituent part of necessary control measures, becomes indispensable nowadays. However, existing methods for information systems auditing are still in the process of development and at this moment no methodology exists. Consequently, basic objective of this work is to develop such computer assisted information system auditing methodology. Foundation of such methodology is application of Benford's Law which links other existing auditing methods. Analysis of literature shows that this field of research is still insufficiently investigated. Therefore, these issues are thoroughly studied, model of methodology is designed, specific methodology is developed, a number of tests and other examinations are performed, methodology is checked on representative sample and recommendations for further development of information systems audit activities and corresponding auditing software tools are presented.
A field of research is financial industry (cross border payment system), because major frauds occurred in financial industry segment. These frauds were possible because lack of adequate controls which should have been checked by information systems audit.

Supervisor: Prof. dr. sc. Zdravko Krakar

Appointed members for evaluation and oral examination:
Prof. dr. sc. Josip Brumec
Prof. dr. sc. Ružica Brčić
Prof. dr. sc. Zdravko Krakar
Prof dr. sc. Mario Spremić
Doc. dr. sc. Jasminka Dobša

Oral examination: **Degree conferred:**

The thesis is deposited at the Library of the Faculty of Organization and Informatics, Varaždin

(204 pages, 12 figures, 30 tables, 56 references, original in English)

DD FOI

UDC: 004.05 (043.3)

Current file number:

I. Development of Methodology for Computer Assisted Information Systems Auditing
II. Žgela, M.
III. Faculty of Organization and Informatics Varaždin, Republic of Croatia

IS Auditing
Computer Assisted IS Auditing
Benford's Law
Model of methodology
CAAT

ŽIVOTOPIS

Mario Žgela je rođen 1970. godine u Vinkovcima. Diplomirao je na Fakultetu organizacije i informatike 1993. godine. Na istom fakultetu je 1999. godine magistrirao na poslijediplomskom znanstvenom magistarskom studiju – smjer baze podataka.

Redovito aktivno sudjeluje na stručnim i znanstvenim konferencijama kao predavač. Povremeno gostuje kao predavač na Ekonomskom fakultetu u Zagrebu i na Fakultetu organizacije i informatike u Varaždinu.

Od 1994. godine radi u Hrvatskoj narodnoj banci. Voditelj Odjela za razvoj aplikacijskih sustava postaje 1996. godine, da bi 2003. godine bio imenovan izvršnim direktorom Sektora za informatičke tehnologije. Navedenu funkciju obnaša i danas.

Posjeduje stručne certifikate iz područja upravljanja i sigurnosti informacijskih sustava (CGEIT – Certified in Governance of Enterprise IT; CISM – Certified Information Security Manager). Jedan je od osnivača Information Systems Audit and Control Association (ISACA) u Hrvatskoj, njen je dugogodišnji član, a trenutno obnaša i funkciju tajnika.

Radovi objavljeni u međunarodno priznatim časopisima i publikacijama (a1):

1. Krakar Z., Žgela M.: "Application of Benford's Law in Payment System Auditing", JIOS Journal of Information and Organisational Sciences, Vol.3 No.1, 2009., p 39–51

Objavljeni znanstveni radovi (a2):

1. Žgela, M., Krakar, Z.: "Design of Framework for Computer Assisted Information Systems Auditing Methodology (CAISAM)", 20th Central European Conference on Information and Intelligent Systems – CECIS2009 Conference Proceedings, Faculty of Organisation and Informatics, Varaždin, 2009. p. 155-165.

2. Krakar, Z., Žgela M.: "Evaluation of Benford's law application in stock prices and stock turnover", 15th International Scientific Conference "Society and Technology 2008", Zadar, Proceedings, Zadar, 2008., 57–71.

3. Krakar, Z., Žgela, M.: "Application of Benford's Law in Information Systems Auditing", 19th Central European Conference on Information and Intelligent Systems – CECIS

Conference Proceedings, Faculty of Organisation and Informatics, Varaždin, 2008. p.187-201.

4. Krakar Z., Žgela M.: ”CobIT- Framework for IT Governance – Analysis and Experience”, 18th International Conference IIS Information and Intelligent Systems, Varaždin, Proceedings, Varaždin, 2007., 145 -151

5. Žgela, M.: “Some public-key cryptography issues in E-business”, Information and Intelligent Systems 2000, Fakultet organizacije i informatike, Varaždin, 2000., Proceedings, Varaždin, 2000., 174.-185.

6. Žgela, M.: “Active Database Concepts and their Implementation in Oracle8 Database Management System”, Information and Intelligent Systems 1999, Fakultet organizacije i informatike, Varaždin, International Conference, 1999 Proceedings on CD, Varaždin, 1999.